LES ACTES DU FORUM

5E FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ

FIC 2013

Le cyberespace, enjeu de souveraineté et de sécurité

AVEC LA COLLABORATION DU CENTRE DE RECHERCHE DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

SOMMAIRE

Allocution de Manuel Valls 12

Allocution de Fleur Pellerin.....20

Allocution de Kader Arif.....25

P1 – Le continuum défense-sécurité
dans le cyberespace.....30

P2 – Cyberespace, identité
numérique, éthique et vie privée.....50

P3 – Quelle politique industrielle
en matière de cybersécurité ? 73

P4 – Le traitement judiciaire de la
cybercriminalité à l'échelle européenne
et internationale : quelles perspectives ? 92

A1 - Géopolitique du cyberespace.....110

A2 - Souveraineté et Cloud
computing 112

A3 - Clusif - Panorama de la
cybercriminalité, année 2012 115

A4 - Cyberdélinquance ou cybercriminalité organisée :
Quels sont les profils des cybercriminels ?.....118

A5 - Cybersécurité et continuité des services publics 121

A6 - Nouvelles formes de
conflictualités dans le cyberespace 124

A7 - Gouvernance du cyberespace 127

A8 - La modernisation des moyens de prévention et d'investigation dédiés au traitement des infractions cybercriminelles.....130

A9 - Cyberespace et contrefaçon 132

A10 - La cybersécurité des systèmes industriels.....135

A11 - DRH et cybersécurité : quelles obligations pour l'employeur et le salarié ? 138

A12 - Smart cities : Quelle sécurité pour les villes de demain ? 141

A13 - OTAN, UE ...: quelles alliances en matière de cybersécurité et de cyberdéfense ? 144

A14 - Existe-t-il un marché pour la cybersécurité ?.....147

A15 - De l'activisme à l'hacktivisme 149

A16 - Quel parcours pour les particuliers et les entreprises victimes d'actes criminels ? 151

A17 - Cybersécurité : quels enjeux pour les SCADAS énergétiques ? 153

A18 - Les APTs (Advanced Persistent Threat) : vraie menace ou coup marketing ? 156

A19 - Dématérialisation et archivage 158

A20 - Technologies de l'information et de la communication et ordre public.....160

A21 - Droit du cyberespace : entre réactivité et proactivité de la loi.162

A22 - Usurpation d'identité : quels risques ? Quelles solutions ? 165

SOMMAIRE

A23 - Outsourcing : comment
externaliser en toute sécurité ?.....167

A24 - Recrutement, formation et
entraînement des professionnels de la cybersécurité 169

A25 - Les Collectivités Territoriales face aux risques numériques.....171

B1 - Cyber terrorisme : mythe et réalité.....176

B2 - Sécurité des télécommunications 179

B3 - Plans de continuité et reprise d'activité :
la question du retour en mode dégradé 182

B4 - Cybercriminalité bancaire et financière 184

B5 - E-réputation : quels risques pour
les entreprises et les particuliers ? 187

B6 - Nouvelles technologies,
nouveaux usages, nouveaux risques 190

B7 - Cybersécurité et santé.....193

B8 - Regards croisés sur les stratégies de cyberdéfense.....196

B9 - Développement informatique sécurisé
comment intégrer la sécurité en amont ? 198

B10 - La résilience internet 201

B11 - Monétique et commerce en ligne
quelle sécurité pour les nouveaux moyens de paiement ? 203

B12 - Quelle politique de sécurité des
systèmes d'information adopter en entreprise ? 205

B13 - Quelle politique de sécurité pour le système d'information
des collectivités territoriales ? 207

B14 - Lutte informatique défensive et Security Operation Center :
vers une cybersécurité dynamique.....210

B15 - BYOD, réseaux sociaux...
Les nouveaux risques en entreprises.....213

B16 - Le management des
professionnels de la cybersécurité.....216

B17 - La cybercriminalité, un risque assurable ? 219

B18 - Open data, libération des données
publiques et sécurité 221

B19 - Développer des réseaux de
résilience à l'échelon territorial 223

Communiqué de presse
Manuel VALLS et Fleur PELLERIN 226

EDITORIAL

Alors que plus aucun processus de notre société ne peut fonctionner sans des systèmes d'information et réseaux numériques fiables et sûrs, l'insécurité informatique s'aggrave et s'étend jusqu'aux entreprises et administrations les mieux protégées. Les attaques informatiques deviennent incessantes et très sophistiquées, perpétrées par des hackers, des commandos du numérique, de plus en plus ingénieux et organisés. Comme l'océan dans les temps anciens, le cyberespace, qui apporte tant à la société et à l'économie, est devenu le nouveau territoire de chasse des pirates, corsaires et autres flibustiers.

Les activités que services publics et entreprises y conduisent doivent y être mises en sécurité, protégées et défendues ; aucune n'est à l'abri d'une agression, parfois grave, dont les auteurs resteront souvent à tout jamais anonymes.

Dans ce contexte, la cybersécurité est devenue un enjeu essentiel pour la Nation. La confiance du citoyen, du consommateur, de l'opinion dépend d'un fonctionnement harmonieux de la société, et donc des systèmes d'information qui en sont au cœur. Compte tenu des enjeux régaliens et du caractère stratégique de la sécurité des systèmes d'information qui concerne les organismes les plus sensibles de l'Etat au même titre que les acteurs économiques, pouvoirs publics et entreprises doivent plus que jamais travailler ensemble pour faire face aux cybermenaces toujours plus sophistiquées.

Selon le référentiel général de sécurité français, 80% des attaques informatiques peuvent être bloquées par une bonne « *hygiène informatique* » et des mesures de sécurité préventives. 19% des attaques sont détectées à l'aide de dispositifs proactifs de surveillance des réseaux et de détection des agressions. Ce sont ainsi 99% des attaques qui peuvent être parées par une approche globale de la cybersécurité. Quant aux attaques les plus sophistiquées, s'il est impossible de s'en prémunir à coup sûr, l'entreprise peut considérablement limiter leur impact si elle s'est dotée d'une sécurité en profondeur et s'est bien préparée à gérer la crise. Ce qui, en outre, facilitera l'identification et la poursuite judiciaire des agresseurs.

J'observe qu'un nombre croissant d'organismes publics et d'entreprises prennent en compte ce besoin de sécuriser leur activité. De plus en plus, les dirigeants prennent conscience des enjeux et, bien que les budgets soient rares, tiennent à mettre en place des approches cohérentes et globales des questions de cybersécurité.

Le Forum International de la Cybersécurité répond à cette tendance croissante qui veut que la cybersécurité soit approchée de manière professionnelle, cohérente et globale. Depuis 2007, la Gendarmerie nationale nous offre cette occasion de rencontre entre acteurs de la sécurité, mêlant les cultures publiques et privées, les spécialistes et les décideurs. Encouragée cette année par la région Nord-Pas de Calais et organisée par CEIS, ce forum a offert de très nombreuses occasions de partager les approches et les savoir-faire, de progresser dans la sécurité du cyberespace.

La participation de près de 2400 acteurs publics et privés au 5ème Forum International de la Cybersécurité a été une excellente occasion de progresser sur le chemin de la sécurité numérique et, pour l'avenir, facilitera une navigation sûre dans les eaux dangereuses – mais fécondes – du cyberespace !

Luc-François Salvador
Président-Directeur Général
du groupe Sogeti
Membre du Comité Exécutif
de Capgemini

5e Forum international de la cybersécurité

Lille – lundi 28 janvier 2013

Mots d'accueil
Pierre DE SAINTIGNON

Mesdames et messieurs, monsieur le Préfet, monsieur le Ministre qui nous vient du Cameroun, je suis très honoré de votre présence. Mon Général, je suis très heureux de participer à l'ouverture du FIC en tant que premier Vice-Président de la région en charge de l'Économie et premier adjoint au maire de Lille.

Alors autant vous dire que nous somme très heureux de vous savoir aussi nombreux, à l'occasion de ce Forum international de la cybersécurité, au cœur de notre capitale historique des Flandres et de la région Nord Pas-de-Calais mais aussi, pour deux jours, capitale mondiale de la cybersécurité et de la confiance numérique.

Nous serons 2 400. Quelques 80 journalistes nous rendrons visite au cours de ces deux jours. Nous recevons 379 partenaires et exposants, 225 intervenants et 52 pays. La représentation s'établit à peu près de la manière suivante : 30 % de décideurs publics des États, à la fois des services des États et de leur collectivité locale, 50 % d'entreprises dont 60 % de grande taille, 10 % de grandes écoles et d'universités et, question tout à fait essentielle pour ce qui nous concerne, 10 % d'invités ou de participants associatifs ou qui agissent dans ce champs.

Je vous remercie très chaleureusement de votre présence et vous convie à ces débats qui seront aussi nombreux que riches. Mon général, la réussite de cet événement ambitieux, qui a nécessité une grosse préparation, repose sur vous, sur nous et ceux qui interviendront. En tous les cas, le gouvernement français ne s'y est pas trompé puisque Manuel VALLS, le ministre de l'Intérieur, nous rendra visite ainsi que Jean-Yves LE DRIAN, ministre de la Défense, Fleur PELLERIN, le ministre délégué auprès du ministre du Redressement Productif en charge précisément des questions liées à l'économie numérique.

Alors pourquoi Le FIC à Lille ? D'abord mon général, parce que nous en avons eu l'idée il y a six ans et qu'avec beaucoup de ténacité, beaucoup d'engagement, parfois dans l'adversité, nous avons su maintenir les quatre premières. Notre choix en organisant cette cinquième édition est d'ancrer définitivement le FIC dans le rendez-vous de notre région, le rendez-vous donné au monde sur ces questions aussi stratégiques. Revenant il y a

quelques minutes d'un voyage économique en Chine, je puis vous dire à quel point ces questions sont absolument déterminantes.
Aujourd'hui, la cinquième édition représente une étape particulièrement importante dans le contexte d'une manifestation renforcée qui se veut être un lieu de connaissance, de rencontre et d'échanges sur les solutions. Rien n'aurait pu se faire sans le Conseil régional, bien sûr, mais aussi sans la Gendarmerie nationale et l'apport déterminant du CEIS et d'Euratechnologies qui sont nos deux partenaires
avec la mission « *Eurométropole défense-sécurité* », animée par le général THOMANN. Cela constitue une équipe impressionnante, extrêmement diversifiée et qui a en commun cette ambition qui nous réunit pendant ces deux jours. Le soutien du Conseil régional témoigne de la grande
ambition que nous avons de faire de la région Nord Pas-de-Calais, une référence mondiale en matière de cybersécurité. C'est une ambition partagée par l'ensemble des acteurs économiques et sociaux de notre région qui sont réunis dans ce que l'on appelle le « *schéma régional de développement économique* ». Il s'agit d'une construction très nordiste où tous les acteurs sociaux, économiques, politiques et consulaires sont ensembles, main dans la main, pour réfléchir à leurs difficultés et résister parfois à la crise. Elle a également vocation à concevoir notre avenir et organiser notre futur et c'est dans ce cadre-là, naturellement, que le FIC prend toute sa place. On ne peut pas, en effet, parler de développement économique sans parler de protection de nos entreprises, d'intelligence économique et donc de cybersécurité et de confiance numérique. On ne peut pas parler des nouvelles technologies ou de celles qui ne sont plus complètement nouvelles, sans parler de protection des données stratégiques si essentielles à notre compétitivité et à notre intelligence collective. Les cybermenaces qui nous entourent nous obligent à une capacité d'anticipation et nous obligent à des moyens de riposte. C'est la culture de la confiance numérique que nous voulons diffuser au travers de cet événement et je suis en mesure de vous annoncer la création d'un cluster régional qui s'appellera pour le moment « *Cybersécurité et confiance numérique* ». Il réunira l'ensemble de nos partenaires et s'appuiera naturellement sur les pôles déjà existants, le pôle d'excellence ubiquitaire qui est piloté ou coordonné par Eura technologies mais aussi le pôle numérique régional et naturellement l'Association RD2SI, Euratechnologies, les universités et les centres de recherche. Ce pôle pourra mettre ses compétences au service des entreprises, au service des collectivités et témoigner de notre savoir-faire bien au-delà des frontières du Nord-Pas-de-Calais. Naturellement, ce pôle est l'annonce de ce que nous ferons à partir du second semestre

« On ne peut pas, en effet, parler de développement économique sans parler de protection de nos entreprises, d'intelligence économique et donc de cybersécurité et de confiance numérique.»

2013 puisque nous l'avons décidé et qu'il nous reste six mois pour le construire, le définir, l'organiser. Pour l'heure, c'est la session 2013 du FIC que je voulais saluer en vous souhaitant de très bons travaux, en vous disant par avance qu'on se retrouvera à peu près à la même époque l'année prochaine pour un FIC nouveau qui tiendra le plus grand compte de ce que nous aurons fait au cours de ces deux jours.

Je vous remercie de votre attention et je passe la parole au général WATIN-AUGOUARD.

Général d'Armée (2S)
Marc WATIN-AUGOUARD

Monsieur le président, monsieur le préfet, monsieur le ministre, messieurs les officiers généraux, mesdames et messieurs, Le général d'armée Jacques Mignaux aurait aimé être parmi nous ce matin pour prononcer ces mots d'accueil. Mais l'actualité nationale l'oblige à participer à une importante réunion. Le directeur général de la gendarmerie nationale nous rejoindra dans la journée. Il m'a demandé de vous accueillir en son nom.

Je le fais avec plaisir parce que le FIC est né à Lille, vous le savez, au début de l'année 2007. Il est né parce qu'il y avait des pionniers, notamment Régis Fohrer et Corinne Objois. A cette époque, il n'était pas encore question des attaques massives qu'a connues l'Estonie. Le Livre Blanc sur la défense et la sécurité nationale n'avait pas encore placé la cyberdéfense au rang des priorités. Le FIC est né à Lille, il a grandi à Lille, trop vite peut-être

puisqu'il est entré dans un « sommeil actif » après sa quatrième édition. Aujourd'hui, le cinquième Forum sur la cybersécurité renaît à Lille. Ce n'est pas un hasard, ce n'est pas une opportunité, c'est un choix légitime, un choix de fidélité.

Dès le début, la région Nord-Pas-de-Calais a partagé notre aventure, au point de devenir aujourd'hui un partenaire essentiel avec CEIS et Euratechnologies. Ce Forum se tient à nouveau à Lille, il restera à Lille!

Ce n'est pas un salon, ce n'est pas un colloque, c'est un forum ouvert, décloisonné. Il est ouvert sur l'international parce que la cybersécurité est tributaire d'une coopération internationale renforcée. Une quarantaine de pays sont ici représentés, ce qui démontre bien que la cybersécurité n'est pas seulement un enjeu franco-français, ni un enjeu européen, mais un enjeu mondial. Merci monsieur le Ministre d'être présent! Vous êtes en quelque sorte le chef de file de toutes les délégations internationales qui sont aujourd'hui parmi nous et que je salue. Forum ouvert sur le monde, le FIC est aussi un lieu de décloisonnement. L'action solitaire est vaine dans le cyberespace. Nous devons décloisonner l'action des services de l'État qui doivent travailler ensemble, mieux travailler ensemble. Nous devons aussi favoriser la convergence entre l'action du secteur public et celle du secteur privé. Personne ne possède à lui seul la réponse aux menaces et aux risques qui pèsent sur cet espace de liberté. La sécurité sur le cyberespace ne se conjugue pas avec le« *je* », avec le « *tu* », ni avec le « *il* »; elle se conjugue avec le « *nous* », « *nous* », tous ensemble c'est-à-dire, ici les 2 400 inscrits représentants toutes les professions, toutes les administrations, toutes les collectivités, toutes les entreprises qui veulent préserver l'extraordinaire opportunité qu'offre le cyberespace en termes d'accès à la culture, au développement économique, à la communication. Nous sommes ici rassemblés pour partager de la compétence, de la connaissance. Mais nous devons aussi partager une même conscience. Répondre à la question « *comment ?* », c'est bien ! Mais il faut aussi répondre à la question « *pourquoi ?* ».

Quel sens veut-on donner à l'avenir du cyberespace ? Sommes-nous désireux de créer une éthique du cyberespace, une conscience « *cybercitoyenne* » ? Rien ne servirait à l'Homme de gagner le cyberespace, s'il venait à y perdre son âme. C'est cela « *l'esprit FIC* », l'état d'esprit du FIC. C'est un état d'esprit animé par le réalisme mais aussi porteur de confiance. Je souhaite que ce 5ème FIC contribue à répondre à ces questions essentielles. Agissons ensemble pour rester les maîtres d'un cyberespace encore inachevé, sinon chacun de nous subira dans la solitude! Tel doit être le fil conducteur des séances plénières et des ateliers auxquels nous allons participer!

Mesdames et messieurs, je vous souhaite un bon FIC 2013!

Allocution de Manuel valls

MINISTRE DE L'INTÉRIEUR

Mesdames et Messieurs,

Il m'appartient de clore cette 5e édition du forum international de la cybersécurité. Un forum dont la réputation n'est plus à faire et qui, en l'espace de deux jours, vous a permis d'appréhender, mieux encore, tous les aspects que recouvrent la question de la cybersécurité : protection des citoyens, des services publics, des entreprises. Nous le savons tous ici : les menaces liées à l'essor d'Internet n'ont rien de virtuel. Elles sont bien réelles ! Sur le réseau, se déploie une criminalité d'une forme nouvelle. Une criminalité, particulièrement efficace, qui peut mettre en péril des pans entiers de notre économie, de nos systèmes de décision et de gestion et donc de la souveraineté des Etats. J'interviens donc pour clore vos échanges. Clore ne me semble toutefois pas le verbe adapté, car dans ce domaine de la cybersécurité, il nous reste beaucoup à faire. Et je sais que, dès demain, chacune et chacun d'entre vous, de retour dans vos entreprises, vos administrations respectives, aurez à cœur de toujours progresser. Beaucoup reste à faire, même si je n'ignore pas que beaucoup a déjà été fait. Et je veux saluer, à nouveau, ce partenariat qui s'est établi entre la Gendarmerie nationale – belle démonstration de sa modernité ! – la Région Nord Pas-de-Calais et le monde de l'entreprise. Ce partenariat qui rassemble service public de la sécurité, collectivité territoriale et secteur privé – et qui se reflète dans la richesse des intervenants et des participants présents à ce forum – traduit, à lui seul, la diversité des menaces liées à la révolution numérique. Une révolution qui ne doit pas se faire au détriment des plus faibles, des personnes les moins informées, des organisations les moins solides. Pendant ces deux journées, les échanges de bonnes pratiques ont été encouragés. Je sais que de nombreux axes d'action ont émergé de vos réflexions.

Si le FIC a une telle notoriété, il le doit à sa dimension internationale : 40 nationalités sont ici représentées. Cette coopération entre les pays est nécessaire pour lutter contre une criminalité qui ne connaît aucune frontière. Une cybercriminalité organisée,

en pleine évolution, réclame une action mieux coordonnée entre les pays. Les formes actuelles de la cybercriminalité, vous le savez, sont très diverses : atteintes aux systèmes de traitement automatisés des données, escroqueries avec récupération des données personnelles, atteintes sexuelles aux mineurs, traites des êtres humains, proxénétisme, usurpation d'identité, contrefaçons, y compris de médicaments. Toutefois, ces formes sont appelées à évoluer. L'augmentation du nombre de connexions, le progrès des technologies – les savoirs servent aussi les mauvaises intentions ! – ne peuvent qu'accroître les risques. Nous devons donc savoir anticiper ces évolutions. Par ailleurs, la discrétion voire l'anonymat permis par Internet, la difficulté à établir des preuves, la facilité d'utilisation, les profits rapides et élevés, sont autant de facteurs aggravants. La cybercriminalité est, pour les auteurs, bien plus rentable et bien moins risquée que les formes traditionnelles de délinquance. Si les mobiles des délinquants restent les mêmes (vengeance, jalousie, envie, perversité), l'appât du gain constitue le principal facteur explicatif du passage à l'acte. La criminalité sur Internet est devenue une criminalité industrialisée, organisée et mondialisée, avec ses fournisseurs de services, ses virus « clés en main », ses entreprises innovantes, ses intermédiaires, ses fournisseurs de fichiers de coordonnées bancaires ou d'adresses mail. Les données recueillies par les pirates font l'objet d'une véritable économie souterraine avec ses réseaux qui opèrent, vous le savez, en Europe de l'est, aux Etats-Unis, en Chine ou en Allemagne. C'est ainsi une véritable e-division internationale du travail qui s'est mise en place avec des « *apprentis* » et des « *vrais* » pirates informatiques, des intermédiaires qui prêtent leurs comptes aux cyberdélinquants ou encore des individus qui transforment les gains virtuels en argent réel.

La réponse que nous devons apporter doit être très structurée, organisée tant au plan national, qu'européen et international. Je connais la volonté réelle de coopération – ce forum en est la preuve – mais aussi les difficultés, parfois les résistances, pour construire cet ordre juridique et judiciaire international. Certes, nous disposons de textes pour lutter contre la cybercriminalité. Mais ils sont trop nombreux. Si je prends l'exemple de la France, ces textes sont disséminés dans cinq codes différents, sans compter le code de procédure pénale ni les lois non codifiées. Un effort de réunification des normes, de simplification, d'adaptation et de mise en cohérence est donc nécessaire, tant au plan national qu'international. Le Conseil de l'Europe a adopté, en 2001, la convention de Budapest sur la cybercriminalité. Il s'agit du premier traité international dans ce domaine qui vise à harmoniser les législations nationales sur les infractions pénales commises au moyen des réseaux numériques. Il nous faut aller plus loin. Il nous faut, également, mieux coordonner l'action entre les services chargés de lutter contre la cyberdélinquance. A ce titre, je salue l'ouverture, le 11 janvier dernier, du centre européen de lutte contre la cybercriminalité (EC3) qui mutualisera les moyens et apportera un soutien opérationnel très utile aux services dans chacun des

Etats membres de l'Union européenne. Combattre la cybercriminalité impose de se doter des outils adaptés. Pour agir plus efficacement contre un phénomène, il faut d'abord bien le connaitre. Or, malgré les efforts accomplis, nous ne disposons pas encore, en France, d'une vision précise des infractions liées au cyberespace. C'est pourquoi, comme je l'ai annoncé il y quelques jours, la refonte de l'outil statistique de suivi de la délinquance, mise en œuvre avec l'Observatoire national de la délinquance et des réponses pénales (ONDRP), prévoit la création d'un indicateur « cybercriminalité ». Cet indicateur dédié permettra de rendre compte de cette délinquance et d'en suivre les variations. Cette évolution sera complétée par le déploiement d'un nouveau logiciel d'enregistrement des plaintes dans les commissariats de police – la gendarmerie a déjà accompli sa migration – qui permettra le recensement de toutes les cyberinfractions. La généralisation de la plainte en ligne contribuera, également, à diminuer le phénomène d'évaporation concernant les infractions qui ne sont pas actuellement portées à la connaissance des forces de sécurité. Mieux connaître la cyberdélinquance doit nous permettre de mieux y faire face. Il nous faut tout d'abord – et de manière urgente ! –, réorganiser, mettre en ordre et adapter notre droit matériel et processuel. Nous devons, également, organiser et coordonner les interventions des multiples intervenants. Plusieurs acteurs agissent, en effet, en matière de lutte contre la cybercriminalité : l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), l'office central de répression des violences aux personnes (OCRVP), la direction centrale du renseignement intérieur (DCRI), la brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI), la brigade de protection des mineurs de Paris (BDM), l'institut de recherche criminelle de la gendarmerie nationale (IRCGN), le service technique de recherches judiciaires et de documentation (STRJD). Nous devons permettre une action globale et plus cohérente au sein du ministère de l'Intérieur. Une action qui doit se faire en lien avec les services des douanes et de la répression des fraudes. Compte tenu des évolutions technologiques constantes et rapides, la formation des personnels qui luttent contre la cyberdélinquance a une dimension stratégique. Des efforts notables ont été accomplis par la police et la gendarmerie. Toutefois, la cybercriminalité nous oblige à penser autrement nos critères de formation et de recrutement. Il nous faut, enfin, repenser certains grands équilibres. D'abord entre protection de la vie privée et sécurité. La loi du 6 janvier 1978 « *informatique et libertés* », puis la loi sur la fraude informatique, en 1988, « *loi dite Godfrain* » [dont je salue la participation de son auteur à ce forum] ont été suivies de huit autres lois pénales relatives à Internet.

Désormais, le numérique est partout dans notre société. Nous sommes tous, citoyens, entreprises, administrations, utilisateurs des outils numériques et connectés entre nous, à partir de nos téléphones, de nos ordinateurs et bientôt de nos véhicules. Se pose donc, de façon cruciale, la question de la protection de nos vies privées et de notre identité. Nous devons intégrer

la décision du Conseil constitutionnel du 22 mars 2012 concernant la loi sur la protection de l'identité. Vous le savez, la mise en place d'un fichier commun aux cartes nationales d'identité et aux passeports comportant des données biométriques, tout comme l'accès donné aux fichiers aux services anti-terroristes ont été censurés. Dès le mois de novembre, j'ai donc saisi l'inspection générale de l'administration afin de réfléchir à une architecture d'ensemble de sécurisation des titres et de leur exploitation. Ses conclusions sont attendues à la fin du mois de février. J'ai également proposé à la garde des Sceaux d'entamer une réflexion conjointe, préalable à un projet de loi « *Habeas corpus numérique* ». Plusieurs sujets de réflexion doivent être traités conjointement. Ils concernent, notamment, les modalités d'accès des personnes aux données des fichiers de police qui les concernent, les garanties législatives encadrant la création des fichiers de police ou encore le droit de disposer des traces ou des empreintes numériques. Nous devons, ensuite, penser l'équilibre entre liberté d'expression et sécurité. Le déferlement, sur les réseaux sociaux, de messages antisémites, homophobes, ou encore la diffusion récente de l'image de la dépouille d'un de nos soldats assassiné en Somalie, soulèvent la question de la liberté d'expression sur Internet. L'enjeu est simple : comment faire respecter par les fournisseurs d'accès et les hébergeurs le droit national auquel ils opposent le droit américain ? A ce titre, la décision prise par la justice française demandant à une plateforme de microblogging de communiquer les données permettant d'identifier les auteurs de propos racistes et antisémites est une avancée. Mais un travail doit se poursuivre permettant l'approfondissement des relations entre l'Etat et les opérateurs. Je n'exclus pas la mise en place de chartes de bonne conduite ; c'est souvent un préalable efficace à l'application pleine et entière de nos lois nationales.

De façon générale, le traitement de certains délits de presse (apologie du terrorisme, incitation à la haine raciale, au meurtre, propos racistes, antisémites ou homophobes) doit pouvoir être repensé sans toucher, bien entendu, aux grands équilibres de la loi sur la presse de 1881. Clairement, la question est posée, aujourd'hui, compte tenu de la force de frappe d'Internet et de son influence sur les populations, de savoir si la répression de tels messages relève encore de cette législation. Enfin, nous devons repenser l'équilibre entre libertés individuelles et sécurité L'émergence de menaces nouvelles et notamment celles du cyber-djihadisme nous obligent à adapter notre arsenal juridique. Je veux un Etat protecteur. Protecteur de la vie privée, de la liberté d'expression, des libertés individuelles y compris en organisant les conditions juridiques de leur limitation, dès lors que la sécurité de nos concitoyens est en jeu. Je me suis récemment exprimé sur ce sujet au Parlement, dans le cadre du vote de la loi anti-terroriste. La présence active de groupes terroristes sur le Net nous oblige, en effet, à doter nos services spécialisés d'outils adaptés. Etendre le champ de l'infiltration numérique, de la captation des données, consolider le socle législatif de la géolocalisation sont autant de nouvelles modalités d'administration

de la preuve qu'il nous faut envisager. Il s'agit de construire une réponse à la mesure des atteintes à nos valeurs perpétrées par ces groupes criminels. Nous avons besoin de nos meilleurs experts pour articuler les exigences de protection des libertés et celle de protection de notre sécurité. Bien entendu, je n'oublie pas le rôle essentiel joué par la CNIL ou encore la CNCIS.
Un groupe de travail interministériel en charge de la lutte contre cybercriminalité
A l'issue des débats sur la loi anti-terroriste, j'ai annoncé l'ouverture, au sein du ministère de l'Intérieur, d'un grand chantier sur la cybercriminalité.
Dès le mois de janvier j'ai lancé ces travaux. D'abord par un déplacement conjoint avec Fleur PELLERIN, il y a 15 jours, au sein des services de police et de gendarmerie en charge de la lutte contre la cybercriminalité ; ensuite avec la proposition de travaux communs faite au ministère de la Justice. Mais je veux aller plus loin encore. J'ai donc décidé la mise en place d'un groupe de travail dédié. Les services des ministères de la Justice et de l'Economie numérique seront, bien évidemment, intégrés à cette réflexion qui se fera, je le souhaite, sous la conduite d'un magistrat. Quatre axes de réflexion me paraissent se dégager : # l'adaptation de notre droit matériel et processuel ; # l'adaptation de nos organisations : nous disposons de services de répression nombreux, efficaces, engagés, mais une plus grande mutualisation des actions s'impose ; # l'adaptation de nos stratégies d'enquêtes et de nos stratégies pénales ; # plus généralement, enfin, l'adaptation de nos stratégies en matière de sensibilisation de nos concitoyens, de formation et de recrutement des professionnels. Je ne doute pas que les réflexions conduites et les propositions faites au cours des deux journées qui s'achèvent, serviront à alimenter ces travaux. Ce groupe de travail aura pour mission de rendre ses conclusions dans un délai resserré. Elles serviront de bases à la définition d'une politique de sécurité intégrant pleinement les enjeux liés à l'Internet. En venant clore ce forum, c'est donc des perspectives que je veux ouvrir. Je veux réaffirmer la détermination du gouvernement à agir pour assurer la sécurité de tous, et donc la cybersécurité de chacun. Je vous remercie.

En effet, bien que déterritorialisé, Internet n'en est pas moins un espace public tout à fait réel. Dois-je rappeler que l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen affirme que la "*liberté*" et la "*sûreté*" sont des droits naturels et imprescriptibles, valables en tout temps et en tout lieu, pour tous les citoyens ?

Pourquoi cette exigence fondamentale ne devrait-elle pas être garantie aussi sur Internet ?

Notre objectif est donc de contribuer à la construction d'un véritable Internet de confiance. La confiance doit être le fondement d'Internet. Pourquoi ? C'est d'abord une exigence politique, au sens général du terme.

J'entends par là l'organisation de la vie collective, ce qui fait une société. Or, cette vie collective passe désormais aussi sur Internet. Les Français sont de plus en plus nombreux à utiliser les réseaux sociaux, à s'exprimer, à débattre sur le Web.

Par ailleurs, plus de 80% de nos concitoyens

ont déjà acheté, ou effectué des démarches administratives en ligne. Et la plupart consultent leur compte bancaire sur Internet.
Deux problèmes viennent immédiatement à l'esprit : la protection de la vie privée et la lutte contre la fraude. Dans les deux cas, la confiance est une condition nécessaire au développement des services en ligne.

C'est parce qu'ils sont convaincus que leur vie privée est protégée que les internautes fournissent des données personnelles. Nous devons donc être vigilants en ce qui concerne les atteintes à la vie privée, la diffusion de fausses informations, les usurpations d'identité, surtout sur les réseaux sociaux.

Sur ce sujet, je suis préoccupée de voir de grands acteurs de l'Internet gérer les don nées personnelles de nos concitoyens de manière unilatérale, dans une transparence limitée, et en dehors de nos frontières.

De même, c'est la confiance qui rend possible le commerce en ligne. Or, le secteur est aujourd'hui touché par des formes de plus en plus diverses de fraude. Nous devons trouver des solutions, notamment via un élargissement et une sécurisation renforcée des moyens de paiement en ligne.

Dans le cadre du développement des technologies NFC, pour le paiement mais aussi pour nombre d'autres usages, le Gouvernement veillera à assurer la sécurité des transactions (dans le cadre des investissements d'avenir, 26 millions d'euros leur ont été consacrés.

La confiance du citoyen, du consommateur doit donc être garantie, parce qu'il en va de notre vie quotidienne à tous, du bon fonctionnement de notre société, et de l'efficacité de notre économie. Ai-je besoin d'insister là-dessus ? Si la sécurité des systèmes

d'information n'est pas assurée, aucune économie moderne ne peut prospérer. Ces principes ne sont pas négociables.

Dès lors, comment garantir et renforcer la confiance numérique ?

Des dispositifs existent déjà, notamment pour lutter contre la fraude et contre les atteintes à la vie privée. Ces dispositifs, quels sont-ils ?
Concernant la fraude, je n'insisterai pas, ce sont des choses bien connues. Pour les transactions les plus risquées, des outils de détection ont été mis en place par les prestataires de systèmes de paiement. Surtout, l'authentification des porteurs ne cesse d'être renforcée – je pense notamment au dispositif 3D Secure. Enfin, la Banque de France informe les usagers sur les risques encourus et les bonnes pratiques à suivre.

En revanche, contre les atteintes à la vie privée et les phénomènes d'usurpation d'identité, beaucoup reste à faire. A ce jour, il n'existe pas en France de projet national d'identité numérique.

Car comment faisions-nous jusqu'à présent ? Amazon, Google, Apple : tous ceux qui ont acheté une application ou une chanson sur l'une de ces plateformes, ou sur leur téléphone Apple ou Google Androïd, ont mis entre les mains de ces sociétés leur identité numérique et leurs données bancaires de manière très peu sécurisée. Nous sommes des millions en France à l'avoir fait.

Vous le voyez, le risque d'une forme de "" de l'identité est déjà avéré dans le monde numérique.

Pourtant, selon moi, pour garantir la protection des données personnelles et de la vie privée sur Internet, une gestion sécurisée des identités numériques est absolument indispensable.

Mesdames, Messieurs, il faut cesser de tergiverser et avancer vers une solution nationale et européenne !
Le Gouvernement entend justement se saisir du problème, combler ce manque et jouer son rôle de catalyseur. Car aucun service public ou commercial agissant isolément n'a la dimension suffisante pour mettre en place, pour ses seuls usages, une infrastructure d'authentification sécurisée à destination du grand public, du fait notamment de son coût.

Le Gouvernement a ainsi annoncé en décembre sa détermination à renforcer la confiance entre les acteurs dans l'espace numérique.

Une doctrine d'identification et d'authentification des utilisateurs et de sécurisation des échanges, fondées sur les usages en vigueur, sera définie pour juin 2013.
J'ai également le plaisir de vous annoncer aujourd'hui le lancement du projet Idénum. Dans le cadre des investissements d'avenir, l'Etat, le Groupe La Poste, Euro-Information, c'est-à-dire le Crédit Mutuel et le CIC, ainsi que PagesJaunes et SFR se sont unis pour créer la société Idénum.
Sa mission sera de fédérer en France le plus grand nombre d'acteurs du Web, afin de définir et de promouvoir des solutions d'identités numériques universelles, pour les professionnels comme pour les particuliers.

Plus précisément, je vous parle ici de solutions d'authentification et de signature, proposées sur différents supports (téléphones mobiles, clés USB, cartes bancaires) et acceptées par tous les sites Web publics et privés qui exigent une garantie d'identité ou une signature électronique.
Ce projet visera à trouver les solutions en phase avec la doctrine définie par l'Etat et c'est tout le sens de la présence de ce dernier au capital de la société Idénum.

Quels sont les avantages du projet Idénum ? Permettez-moi d'insister un peu, mais je crois vraiment qu'il s'agit d'un projet qui va changer beaucoup de choses sur trois plans :

Sur le plan économique tout d'abord, Idénum va contribuer à rendre possible l'Internet de confiance que nous appelons de nos vœux. Les internautes utiliseront encore plus volontiers les services en ligne déjà existants, tandis que naîtront de nouveaux services à haute valeur ajoutée.
Sur le plan social ensuite, Idénum permettra de renforcer la protection des données personnelles, et celle de la vie privée de l'internaute.
Sur le plan politique enfin, cette société devra définir un standard ouvert visant à préserver notre souveraineté nationale face aux alternatives étrangères et non sécurisées.

Surtout, Idénum n'est que la première étape d'un chantier global, qui doit tous nous mobiliser. Je voudrais ainsi qu'elle soit comme une invitation à ce que le secteur de la cybersécurité se structure davantage. La confiance numérique n'en sera que plus forte.

La France souffre d'une absence de véritable

politique industrielle dans le domaine : ses acteurs sont trop dispersés ; sa R&D, insuffisante. Un effort de structuration est donc nécessaire. J'ajoute que le marché de la sécurité des systèmes d'information et des réseaux pourrait représenter 16 milliards d'euros au total en 2014. L'enjeu économique est donc majeur.

Quels sont les objectifs que doit viser cette politique industrielle ? J'en vois trois :

Le premier : favoriser le développement du commerce électronique ;

Le second : faciliter un usage plus large et plus efficace des technologies disponibles pour renforcer la protection de nos entreprises ;

Le dernier : aider les entreprises françaises du secteur à innover et produire de la valeur.

La France possède de nombreux atouts dans le domaine de la cybersécurité, même si on ne le sait pas toujours. Bref, nous n'avons pas à rougir de nos performances sur le marché international, bien au contraire !

Plusieurs de nos fleurons me viennent à l'esprit : Thalès, EADS, Bull, Safran-Morpho, etc. Je pense à Gemalto, Oberthur et Sagem Orga pour les cartes à puce, à Ingenico pour les lecteurs de cartes !

Parallèlement, nous tirons profit d'un très large spectre de compétences – le plus complet d'Europe – grâce à nos nombreuses PME et TPE, qui ne cessent d'innover dans le domaine. La France est ainsi en pointe concernant la cryptologie ou les produits d'analyse de trafic, autant de technologies clés. Nous devons donc encourager ces entreprises à grandir et conquérir de nouveaux marchés, notamment étrangers, dans le respect, bien évidemment, de nos valeurs fondamentales.

En conclusion, l'objectif de cette politique doit être de consolider l'industrie française, déjà très dynamique.

Cela passera par la création d'un environnement de confiance renforcé, et par un effort de structuration du secteur.

Il en va du bon fonctionnement d'un espace dans lequel se déploie notre vie collective, notre vie de citoyens, de créateurs, de consommateurs.

Voilà pourquoi il est, à mes yeux, fondamental que toutes les questions liées à la cybersécurité soient mises sur la table. C'est la meilleure manière de garantir à la fois les libertés fondamentales et l'existence d'un Internet ouvert et sûr.

Je tiens à saluer encore une fois l'initiative du FIC, et je vous souhaite à tous de bons travaux.

Je vous remercie.

Allocution de Fleur Pellerin

MINISTRE DÉLÉGUÉE AUPRÈS DU MINISTRE DU REDRESSEMENT PRODUCTIF, CHARGÉE DES PETITES ET MOYENNES ENTREPRISES, DE L'INOVATION ET DE L'ÉCONOMIE NUMÉRIQUE

Mesdames et Messieurs,

Je voudrais tout d'abord vous remercier pour votre invitation : c'est un véritable plaisir pour moi d'être présente aujourd'hui à Lille à l'occasion du Forum International de la Cybersécurité.

Je tiens également à remercier l'ensemble des participants de cette réunion plénière, dont le thème est complexe et stimulant. "*Cyberespace, identité numérique, éthique et vie privée*" : vaste sujet ! Vous avez tous souligné à quel point il est stratégique et actuel pour nous.

Nous ne pouvons plus attendre pour y répondre ! C'est le message que je suis venue vous transmettre, et vous verrez que le Gouvernement s'est déjà saisi du problème.

Pourquoi la cybersécurité est-elle un secteur crucial ? Tout simplement parce que notre vie quotidienne est de plus en plus dépendante des systèmes informatiques et des données qu'ils exploitent : données médicales, données bancaires, données professionnelles. C'est également le cas de nos entreprises, de nos administrations, de nos usines, bref, de ce qui fait la richesse de la France.

Quand on parle de "*cybersécurité*", on provoque parfois, chez certains, des réactions scandalisées, épidermiques.

Le gros mot, le mot qui disqualifie, finit par être jeté : "*idéologie sécuritaire*" ! Je n'ai pas l'intention de céder aux clichés faciles.

Mon ministère est l'héritier des pionniers du cyberespace. Leur ambition première était de créer un nouvel espace de liberté. Cet objectif est atteint, non pas dans tous les pays, mais en France, c'est l'évidence. Il faut bien sûr rester très vigilant pour qu'il le reste.

Malheureusement, comme dans le monde réel, certaines dérives sur les réseaux peuvent menacer la liberté de tous. Il est bien sûr de la responsabilité de l'Etat d'assurer le maintien de l'ordre public sur Internet pour protéger les libertés et la sécurité de nos concitoyens.

En effet, bien que déterritorialisé, Internet n'en est pas moins un espace public tout à fait réel. Dois-je rappeler que l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen affirme que la "*liberté*" et la "*sûreté*" sont des droits naturels et imprescriptibles, valables en tout temps et en tout lieu, pour tous les citoyens ?

Pourquoi cette exigence fondamentale ne devrait-elle pas être garantie aussi sur Internet ?

Notre objectif est donc de contribuer à la construction d'un véritable Internet de confiance.

La confiance doit être le fondement d'Internet. Pourquoi ? C'est d'abord une exigence politique, au sens général du terme.

J'entends par là l'organisation de la vie collective, ce qui fait une société. Or, cette vie collective passe désormais aussi sur Internet. Les Français sont de plus en plus nombreux à utiliser les réseaux sociaux, à s'exprimer, à débattre sur le Web.

Par ailleurs, plus de 80% de nos concitoyens ont déjà acheté, ou effectué des démarches administratives en ligne. Et la plupart consultent leur compte bancaire sur Internet.
Deux problèmes viennent immédiatement à l'esprit : la protection de la vie privée et la lutte contre la fraude. Dans les deux cas, la confiance est une condition nécessaire au développement des services en ligne.

C'est parce qu'ils sont convaincus que leur vie privée est protégée que les internautes fournissent des données personnelles. Nous devons donc être vigilants en ce qui concerne les atteintes à la vie privée, la diffusion de fausses informations, les usurpations d'identité, surtout sur les réseaux sociaux.

Sur ce sujet, je suis préoccupée de voir de grands acteurs de l'Internet gérer les don nées personnelles de nos concitoyens de manière unilatérale, dans une transparence limitée, et en dehors de nos frontières.

De même, c'est la confiance qui rend possible le commerce en ligne. Or, le secteur est aujourd'hui touché par des formes de plus en plus diverses de fraude. Nous devons trouver des solutions, notamment via un élargissement et une sécurisation renforcée des moyens de paiement en ligne.

Dans le cadre du développement des technologies NFC, pour le paiement mais aussi pour nombre d'autres usages, le Gouvernement veillera à assurer la sécurité des transactions (dans le cadre des investissements d'avenir, 26 millions d'euros leur ont été consacrés.

La confiance du citoyen, du consommateur doit donc être garantie, parce qu'il en va de notre vie quotidienne à tous, du bon fonctionnement de notre société, et de l'efficacité de notre économie. Ai-je besoin d'insister là-dessus ? Si la sécurité des systèmes

d'information n'est pas assurée, aucune économie moderne ne peut prospérer. Ces principes ne sont pas négociables.

Dès lors, comment garantir et renforcer la confiance numérique ?

Des dispositifs existent déjà, notamment pour lutter contre la fraude et contre les atteintes à la vie privée. Ces dispositifs, quels sont-ils ?

Concernant la fraude, je n'insisterai pas, ce sont des choses bien connues. Pour les transactions les plus risquées, des outils de détection ont été mis en place par les prestataires de systèmes de paiement. Surtout, l'authentification des porteurs ne cesse d'être renforcée – je pense notamment au dispositif 3D Secure. Enfin, la Banque de France informe les usagers sur les risques encourus et les bonnes pratiques à suivre.

En revanche, contre les atteintes à la vie privée et les phénomènes d'usurpation d'identité, beaucoup reste à faire. A ce jour, il n'existe pas en France de projet national d'identité numérique.

Car comment faisions-nous jusqu'à présent ? Amazon, Google, Apple : tous ceux qui ont acheté une application ou une chanson sur l'une de ces plateformes, ou sur leur téléphone Apple ou Google Androïd, ont mis entre les mains de ces sociétés leur identité numérique et leurs données bancaires de manière très peu sécurisée. Nous sommes des millions en France à l'avoir fait.

Vous le voyez, le risque d'une forme de "*privatisation*" de l'identité est déjà avéré dans le monde numérique.

Pourtant, selon moi, pour garantir la protection des données personnelles et de la vie privée sur Internet, une gestion sécurisée des identités numériques est absolument indispensable.

Mesdames, Messieurs, il faut cesser de tergiverser et avancer vers une solution nationale et européenne !
Le Gouvernement entend justement se saisir du problème, combler ce manque et jouer son rôle de catalyseur. Car aucun service public ou commercial agissant isolément n'a la dimension suffisante pour mettre en place, pour ses seuls usages, une infrastructure d'authentification sécurisée à destination du grand public, du fait notamment de son coût.

Le Gouvernement a ainsi annoncé en décembre sa détermination à renforcer la confiance entre les acteurs dans l'espace numérique.

Une doctrine d'identification et d'authentification des utilisateurs et de sécurisation des échanges, fondées sur les usages en vigueur, sera définie pour juin 2013.

J'ai également le plaisir de vous annoncer aujourd'hui le lancement du projet Idénum. Dans le cadre des investissements d'avenir, l'Etat, le Groupe La Poste, Euro-Information, c'est-à-dire le Crédit Mutuel et le CIC, ainsi que Pages-Jaunes et SFR se sont unis pour créer la société Idénum.

Sa mission sera de fédérer en France le plus grand nombre d'acteurs du Web, afin de définir et de promouvoir des solutions d'identités numériques universelles, pour les professionnels comme pour les particuliers.

Plus précisément, je vous parle ici de solutions d'authentification et de signature, proposées sur différents supports (téléphones mobiles, clés USB, cartes bancaires) et acceptées par tous les sites Web publics et privés qui exigent une garantie d'identité ou une signature électronique.
Ce projet visera à trouver les solutions en phase avec la doctrine définie par l'Etat et c'est tout le sens de la présence de ce dernier au capital de la société Idénum.

Quels sont les avantages du projet Idénum ? Permettez-moi d'insister un peu, mais je crois vraiment qu'il s'agit d'un projet qui va changer beaucoup de choses sur trois plans :

Sur le plan économique tout d'abord, Idénum va contribuer à rendre possible l'Internet de confiance que nous appelons de nos vœux. Les internautes utiliseront encore plus volontiers les services en ligne déjà existants, tandis que naîtront de nouveaux services à haute valeur ajoutée.

Sur le plan social ensuite, Idénum permettra de renforcer la protection des données personnelles, et celle de la vie privée de l'internaute.

Sur le plan politique enfin, cette société devra définir un standard ouvert visant à préserver notre souveraineté nationale face aux alternatives étrangères et non sécurisées.

Surtout, Idénum n'est que la première étape d'un chantier global, qui doit tous nous mobiliser. Je voudrais ainsi qu'elle soit comme une invitation à ce que le secteur de la cybersécurité se structure davantage. La confiance numérique n'en sera que plus forte.

La France souffre d'une absence de véritable politique industrielle dans le domaine : ses acteurs sont trop dispersés ; sa R&D, insuffisante. Un effort de structuration est donc nécessaire.

J'ajoute que le marché de la sécurité des systèmes d'information et des réseaux pourrait représenter 16 milliards d'euros au total en 2014. L'enjeu économique est donc majeur.

Quels sont les objectifs que doit viser cette politique industrielle ? J'en vois trois :

Le premier : favoriser le développement du commerce électronique ;

Le second : faciliter un usage plus large et plus efficace des technologies disponibles pour renforcer la protection de nos entreprises ;

Le dernier : aider les entreprises françaises du secteur à innover et produire de la valeur.

« La France possède de nombreux atouts dans le domaine de la cybersécurité, même si on ne le sait pas toujours. Bref, nous n'avons pas à rougir de nos performances sur le marché international, bien au contraire ! »

La France possède de nombreux atouts dans le domaine de la cybersécurité, même si on ne le sait pas toujours. Bref, nous n'avons pas à rougir de nos performances sur le marché international, bien au contraire !

Plusieurs de nos fleurons me viennent à l'esprit : Thalès, EADS, Bull, Safran-Morpho, etc. Je pense à Gemalto, Oberthur et Sagem Orga pour les cartes à puce, à Ingenico pour les lecteurs de cartes !

Parallèlement, nous tirons profit d'un très large spectre de compétences – le plus complet

d'Europe – grâce à nos nombreuses PME et TPE, qui ne cessent d'innover dans le domaine. La France est ainsi en pointe concernant la cryptologie ou les produits d'analyse de trafic, autant de technologies clés. Nous devons donc encourager ces entreprises à grandir et conquérir de nouveaux marchés, notamment étrangers, dans le respect, bien évidemment, de nos valeurs fondamentales.

En conclusion, l'objectif de cette politique doit être de consolider l'industrie française, déjà très dynamique.

Cela passera par la création d'un environnement de confiance renforcé, et par un effort de structuration du secteur.

Il en va du bon fonctionnement d'un espace dans lequel se déploie notre vie collective, notre vie de citoyens, de créateurs, de consommateurs.

Voilà pourquoi il est, à mes yeux, fondamental que toutes les questions liées à la cybersécurité soient mises sur la table. C'est la meilleure manière de garantir à la fois les libertés fondamentales et l'existence d'un Internet ouvert et sûr.

Je tiens à saluer encore une fois l'initiative du FIC, et je vous souhaite à tous de bons travaux.

Je vous remercie.

Allocution de Kader Arif

MINISTRE DÉLÉGUÉ AUPRÈS DU MINISTRE DE LA DÉFENSE, CHARGÉ DES ANCIENS COMBATTANTS

Monsieur le Préfet,
Mesdames et Messieurs les élus,
Messieurs les Présidents,
Messieurs les officiers généraux,
Mesdames, Messieurs,

Le Ministre de la Défense, Jean-Yves Le Drian, est finalement retenu à Paris par un contexte dont la gravité est connue de tous. Il vous prie de l'en excuser et m'a demandé d'être avec vous ce matin, pour cette 5ème édition du FIC, le forum international de la cybersécurité.

Je voudrais d'abord en remercier les trois organisateurs : la gendarmerie nationale, qui a eu, en 2007, l'initiative de cet événement important, ainsi que la CEIS, et enfin la région Nord Pas de Calais qui nous accueille cette année.

Je crois que nous sommes tous ici animés par un même constat : la cybersécurité est un sujet dont l'importance est majeure au regard de l'accroissement très rapide de la menace, et dont la complexité, qui dépasse les schémas classiques, nous force globalement certains de nos modes de fonctionnement.

Comme le sénateur Jean-Marie Bockel, que je salue parmi nous, l'a fort bien relevé dans son rapport, la cybersécurité est l'affaire de tous, civils et militaires, acteurs publics et privés, et seule une démarche coordonnée et volontariste permettra de faire face efficacement aux attaques présentes et à venir.

La France a l'ambition de se positionner parmi les nations leaders dans ce domaine, au plan international. Pour ce faire, elle s'est lancée dans une démarche ambitieuse, passant par la mise en place d'une capacité nationale qui soit crédible auprès de nos grands partenaires, par le développement de relations fortes avec ces derniers, enfin par une implication dans les travaux conduits au sein de l'Europe[1] et de l'OTAN. Je tiens à saluer, à cet égard, l'agence européenne de défense qui est présente aujourd'hui.

[1]: L'agence européenne de défense participe à la plénière

Cette crédibilité de la France dans le domaine de la cybersécurité est conditionnée par une triple expertise : celle des acteurs étatiques, celle des acteurs académiques, enfin celle qui est liée aux acteurs industriels.

Je commence par les acteurs étatiques.
L'Agence nationale de la sécurité des systèmes d'information (l'ANSSI), dont j'ai visité le stand à l'instant, est devenue l'autorité gouvernementale en matière de cybersécurité. Elle détient en propre des moyens de veille, de détection et d'intervention qui en font un acteur incontournable du domaine.
Le ministère de l'Intérieur, de son côté, a investi cette lutte de façon décisive, avec ses capacités de renseignement intérieur et de traitement de la cyber criminalité.
Le ministère de la Défense, pour sa part, apporte d'abord un soutien à l'ANSSI, en matière de renseignement spécialisé ou d'expertise technique. Mais il assure aussi, de façon autonome mais toujours en bonne intelligence avec l'ANSSI, la défense de ses systèmes d'informations et la résilience de ceux utilisés pour ses missions militaires.
Puisqu'il m'appartient de représenter le Ministre de la Défense, je tiens à souligner que l'organisation opérationnelle des armées a été récemment ajustée pour y intégrer une chaîne opérationnelle de cyberdéfense, qui soit en cohérence avec le reste. Dans cette perspective, la centralisation au niveau du CPCO, le Centre de Planification et de Conduite des Opérations, garantit aujourd'hui une vision globale mais aussi un tempo rapide permettant de mobiliser tous les moyens nécessaires. Cette chaîne est par ailleurs spécialisée, car elle nécessite des compétences et des habitudes spécifiques, comme pour les autres milieux de combat. Enfin, son action est en partie transverse, car les autres milieux comportent dorénavant une part de cyberespace qui est indissociable.
Alors que cette chaîne opérationnelle de cyberdéfense est maintenant pleinement intégrée au cadre politique et juridique d'emploi des forces armées, l'enjeu est maintenant de poursuivre le développement de leurs capacités à conduire des opérations dans le cyberespace. Mais l'enjeu est aussi d'inscrire ces cyber-opérations au sein des processus d'anticipation stratégique et de planification opérationnelle. ainsi la composante technique confiée à la DGA a pour mission de connaitre et anticiper la menace, de développer la recherche amont, de développer les produits de haut niveau de sécurité, enfin d'apporter une expertise à même de répondre à la crise informatique qui pourrait frapper le ministère de la Défense ou d'autres composantes stratégiques de la Nation.
J'en viens maintenant à la composante industrielle de la cybersécurité, qui a fait l'objet, si j'ai bien compris, de la séance plénière qui vient de se dérouler. Disposer de ce que nous

appelons une base industrielle et technologique de défense performante est absolument essentiel, et d'autant plus dans ce domaine de pointe. Je rappellerais ici que la stratégie du ministère de la Défense, et plus généralement de l'Etat, pour développer cette base industrielle, repose sur plusieurs actions coordonnées :

Coopération avec les grands organismes de recherche comme l'INRIA (l'Institut National de Recherche en Informatique et en Automatique) ;

Soutien de la recherche académique, notamment au travers de financement de thèses de doctorat dont certaines spécifiquement fléchées « *cyberdéfense* » ;

Financement de la recherche au travers des études en amont, dont le montant consacré à la sécurité informatique a doublé cette année et atteindra à court terme 30 à 35 M€ par an ;

Développement, avec nos grands maîtres d'œuvres industriels[2], dont certains sont représentés ici, et acquisition de produits de haut niveau de sécurité à des fins ministérielles et interministérielles, avec l'objectif de permettre aux opérateurs privés d'infrastructures vitales d'en bénéficier également ;

[2]: Thales, Cassidian, Cap Gemini participent à la plénière

Aide, enfin, aux PME innovantes, qui sont nombreuses en France dans ce domaine, au travers de financements d'aide à l'innovation, mais aussi par la signature de conventions bilatérales entre le ministère et les grands maîtres d'œuvre, conformément aux engagements du pacte défense PME annoncé par le Ministre de la Défense le 27 novembre dernier.

Au-delà de cette stratégie, je tiens à vous faire part de la volonté du ministère que je représente de contribuer au développement d'un « *esprit national de cyberdéfense* », à l'image de celui que l'on observe déjà dans un pays comme l'Estonie. A cette fin, nous avons notamment mis en place un réseau de réserve citoyenne cyberdéfense, dont le coordonnateur est Luc-François Salvador[3], qui est également présent aujourd'hui. Ce réseau est particulièrement intéressant ; il transcende notamment les fonctions professionnelles de ses membres pour mettre en place un effort collectif au profit de la cybersécurité.

[3]: Luc-François Salvador, PDG de SOGETI (groupe Cap Gemini) participe à la plénière

Vous l'aurez donc compris, la cyberdéfense, appréhendée de façon globale comme un nouvel espace de confrontation, doit faire l'objet d'une priorité à nulle autre pareille au sein de nos armées. Le renforcement des capacités est ainsi appelé à se poursuivre, en cohérence avec les enjeux croissants de ce domaine de lutte, mais aussi les hypothèses d'emploi des forces militaires et les modèles d'armées.

L'objectif est pour nous d'atteindre une posture interarmées équilibrée et cohérente. Pour ce faire, il va falloir poursuivre notre effort, en combinant des capacités de renseignement et d'appréciation de situation, d'anticipation stratégiques, de planification et de conduite de diverses sortes d'actions cybernétiques. Cette posture, enfin, n'aura de sens que si elle s'insère dans une manœuvre globale et cohérente, qui fasse appel à l'ensemble des moyens d'actions dont les armées disposent.

Voilà les quelques mots que je voulais vous adresser. En remerciant encore les organisateurs de cette 5e édition, je vais poursuivre ma visite, après les stands des principaux acteurs étatiques, par ceux des industriels.

Je vous remercie.

atheos

Le partenaire naturel des stratégies de cybersécurité.

Concevoir

Politiques,
Classification des actifs,
Analyse des risques

Déployer

Dispositifs :
Techniques et Humains,
Organisationnels et Réglementaires

Contrôler

Plan de contrôle
périodique et permanent

Notre Vocation :

" Aider nos clients à concevoir, déployer et contrôler la politique & la stratégie de défense de leur entreprise "

www.atheos.fr

La cyber-sécurité globale

Bull, votre partenaire de confiance dans le cyberespace

Avec Bull, leader européen de la cyber-sécurité globale, analysez vos cyber-risques et pilotez votre sécurité dans une gouvernance unifiée. Maintenez vos systèmes en condition de sécurité avec une défense en profondeur adaptée, anticipez et réagissez immédiatement aux attaques grâce à une défense active.

www.bull.com

P1 – Le continuum défense-sécurité dans le cyberespace

Jean-Claude BOURRET

Mesdames, messieurs, voici donc la première table ronde de ce forum. Première table ronde pour laquelle va participer le général WATIN-AUGOUARD, directeur du centre de recherche de l'École des officiers de la gendarmerie nationale, ancien inspecteur général des armées.
Nous recevons également monsieur Stéphane JANICHEWSKI qui est directeur de la cybersécurité dans le groupe SOGETI, le général Éric BONNEMAISON de la délégation aux affaires stratégiques du ministère de la Défense, Patrick PAILLOUX, directeur général de l'ANSSI et Eduardo RIHAN CYPEL, député, membre de la commission de la défense nationale et des forces armées.
Je vais tout de suite donner la parole au général WATIN-AUGOUARD sur le thème « *qu'est - ce que le continuum défense-sécurité ?* ».

Général d'Armée (2S)
Marc WATIN-AUGOUARD

Le continuum défense-sécurité caractérise l'absence de distance, de séparation entre le domaine de la défense et celui de la sécurité. La défense et la sécurité sont en quelque sorte deux « *sœurs siamoises* ». Elles conservent chacune leur identité, mais un tronc commun les rapproche de plus en plus. Autrefois, on aurait pu parler de contiguïté défense-sécurité dans la mesure où ces deux champs étaient tangents. Aujourd'hui, le continuum met en exergue le fait que certains enjeux relèvent en même temps des questions de défense et des questions de sécurité.
Nous vivions dans un système traditionnellement binaire : guerre/paix, domaine civil/domaine militaire. Progressivement, se construit un système beaucoup plus rhéostatique. A chaque situation doit correspondre une combinaison d'actions, de moyens, à doser en fonction de la nature de la crise. Prenons un exemple qui ne relève pas du cyberespace : celui de la piraterie maritime. Celle-ci relève à la fois du champ de la défense, car elle appelle la mise en œuvre des moyens militaires, c'est le cas de l'opération Atalante, mais elle relève également du champ de la sécurité car sa finalité est d'arrêter des criminels qui agissent en bande organisée et de les déférer devant des juridictions. Il en est de même dans la traque des narco-trafiquants ou, en Guyane,

pour la France, avec la lutte contre les orpailleurs clandestins. L'opération menée est dans tous les cas ambivalente.

En quoi le cyberespace est-il concerné par cette notion de continuum ? Il l'est d'abord par construction, car il a été construit sans frontière avec une infrastructure, ce que l'on appelle la « *couche matérielle* » qui est internationale avec des liens et des nœuds répartis sur l'ensemble de la planète permettant d'acheminer les données, de faire fonctionner les systèmes automatisés de données. Cela favorise une contraction espace/temps qui est extraordinaire. Il n'y a pas un champ de bataille, ni de quartiers sensibles ou de zone de priorité en terme de lutte contre la délinquance. Tout le flux s'imbriquent. Une personne, chez elle, peut être en quelque sorte victime, complice malgré elle, d'une action qui relève de la défense, parce que son ordinateur compromis a servi à une attaque contre une infrastructure critique. La deuxième caractéristique tient aux méthodes qui peuvent être similaires. Les cybercriminels poursuivant des fins crapuleuses, les terroristes ou les « *guerriers* » peuvent avoir recours aux mêmes méthodes aux mêmes « *armes* ». Prenons par exemple le cas d'une attaque par déni de service. Elle peut viser une entreprise pour la faire chanter, des SCADAs pour terroriser la population ou bien des systèmes ministériels ou de commandement dans un but beaucoup plus agressif que l'on pourrait, avec les réserves d'usage, qualifier de « *cyberguerre* » . Finalement, ce qui va distinguer ces actions, c'est leur intensité, leur degré de préparation, de sophistication, l'objectif ciblé et le mobile poursuivi. En fait, ce sont les mêmes armes, les mêmes outils, les mêmes chemins. Dans de nombreux cas, il faut procéder à une analyse des situations pour les qualifier. Lorsque le FBI, la garde civile espagnole et la police slovène arrêtent, dans le cadre de l'opération « *Mariposa* », des individus qui ont compromis près de dix millions d'ordinateurs, ces machines, louées sur Internet, l'ont-elles été pour attaquer un service de commerce en ligne d'une grande entreprise pour la faire chanter, pour troubler gravement l'ordre public par l'intimidation ou la terreur ou bien pour accompagner une attaque massive comme celle qu'ont connue l'Estonie ou la Géorgie ?
Nous sommes dans un système dont la polyvalence permet des applications très différentes. Voilà pourquoi le cyberespace est un espace au sein duquel les acteurs liés à la défense et ceux qui sont dédiés à la lutte contre la cybercriminalité peuvent être engagés simultanément. La lutte contre la cybercriminalité ne s'arrête pas là où commence la cyberdéfense. A un moment donné, elles sont parfaitement imbriquées, notamment parce que la défense des intérêts fondamentaux de la Nation, qui est protégée par le Code pénal rejoint la protection des systèmes de traitement automatisés de données organisée dans ce même code par la loi GODFRAIN.
De ce continuum, nous pouvons déduire quelques conséquences. En premier lieu, dans un continuum défense-sécurité, l'État doit s'organiser, se mette en ordre de bataille. On le voit depuis 2008, avec la montée en puissance de la cyberdéfense avec la création et le renforcement de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). La création d'une composante cyberdéfense au sein de l'état-major des armées complète ce dispositif en l'étendant au champ des opérations militaires. La colocalisation prochaine de leurs centres opérationnels va dans le sens de la cohérence et de la complémentarité.

Mais il faut aussi que du côté du « », c'est-à-dire de la justice, de la police, de la gendarmerie et des douanes, une démarche similaire de mise en cohérence soit entreprise et que les liens avec la cyberdéfense soient renforcés. Il faut donc une plus grande interconnexion, une approche régalienne plus maillée, parce qu'à un moment donné ce qui relève de la cyberdéfense peut intéresser ce qui concerne la lutte contre la cybercriminalité.
La deuxième conséquence concerne le renseignement. Les attaques ne sont jamais découplées de ce qui se passe dans le monde réel. Les services de renseignement civils et militaires doivent collaborer davantage, notamment en mutualisant les moyens techniques. Mais le renseignement doit aussi intégrer toutes les informations qui proviennent du secteur privé. Les services spécialisés doivent également être mieux connectés avec les acteurs de terrain, les policiers, les gendarmes, les douaniers qui dans la « *capillarité* » de leur réseau territorial sont des récepteurs de signaux faibles ou même de signaux forts qui ne sont pas souvent exploités.
La troisième conséquence concerne les ressources humaines. Ce sont souvent les mêmes hommes, les mêmes femmes qui peuvent un jour agir dans le cadre de la lutte contre la cybercriminalité et un autre jour au service de la cyberdéfense. Il faut donc réfléchir sur le recrutement, la formation, les cursus de carrière.
Le quatrième point porte sur la recherche et le développement. Cette question s'inscrit pleinement dans une politique industrielle. Le cyberespace fait appel à des technologies duales. La recherche de la traçabilité des attaques intéresse aussi l'enquêteur confronté à une démarche forensique de recherche des preuves matérielles de l'infraction. Tout ce qui est découvert par les uns est utile aux autres.

Autre conséquence du continuum, la nécessité de revoir le corpus juridique en évitant sa dispersion. Il faut un droit qui couvre l'ensemble du champ, de la cyberdélinquance jusqu'au haut du spectre de la cybercriminalité. Le discontinuum est marqué par l'application du droit des conflits armés qui n'est pas adapté aux conflits dans le cyberespace.

Enfin, dernière conséquence du continuum, c'est l'unité de l 'action diplomatique au service d'une stratégie de cybersécurité qui intègre aussi bien la coopération militaire que celle en matière de sécurité intérieure.

Jean-Claude BOURRET

Merci mon général. Tous les jours, nous constatons, quand nous sommes devant nos écrans d'ordinateurs, la fragilité des systèmes de protection. Tous les jours, on découvre des failles de sécurité qu'il faut corriger. Ma question est la suivante: « *pensez-vous qu'il y ait dans toutes les armées du monde et en particulier dans l'armée française suffisamment de personnel qualifié pour faire face à ce genre de menace* » ?

Général d'Armée (2S)
Marc WATIN-AUGOUARD

S'agissant de la première question, je pense qu'elle relève des compétences de Patrick PAILLOUX qui est le mieux qualifié pour répondre. S'agissant de la seconde, nous devons mieux maîtriser l'usage des réseaux sociaux au sein des armées, notamment lorsqu'elles sont engagées dans des opérations. Une image apparemment anodine peut révéler à l'adversaire un dispositif, la nature des moyens ou des armements engagés.

Jean-Claude BOURRET

Nous sommes confrontés à l'irresponsabilité de certains qui ne comprennent pas que dès l'instant où l'on est sur le web, c'est la totalité du monde qui a accès à l'information.
Mon général, je vous remercie. Monsieur JANICHEWSKI, vous êtes directeur des activités de cybersécurité au sein du groupe SOGETI et vous êtes également ingénieur général de l'armement. Une question pour démarrer votre intervention si vous le voulez bien : « *quel est le point de vue d'un industriel comme SOGETI sur ces questions que et quelle contribution pouvez-vous apporter pour la défense et la sécurité nationale ?* ».

Stéphane JANICHEWSKI

Le point de vue d'un industriel est le point de vue, je dirais, d'un prestataire de service qui peut aider les organismes publics ou privés à mieux se défendre contre les cyberattaques. Première remarque sur le continuum : d'un point de vue strictement technique, les attaques utilisent le même cadre, c'est-à-dire le cyberespace, et sont de même nature. De ce fait, la manière de se protéger, que ce soit pour un organisme public ou privé, va être la même et de ce point de vue je ne saurais trop aller dans le sens de ce qui vient d'être dit sur le caractère dual de la cyberdéfense. Ce qui peut changer simplement, c'est le contexte. Dans un cadre civil, l'objet des attaques ou l'objectif des attaques peut être évidement de nature différente de ce qui vise des actifs de souveraineté. Un contexte militaire, lors d'un conflit ouvert déclaré, va permettre évidement d'agir de manière complètement différente puisque l'ennemi, l'origine, la source de l'attaque sont beaucoup plus faciles à identifier. Dans le cadre d'une approche technique, tout est parfaitement dual. Ce qui va changer c'est l'organisation pour mettre en place la défense. De ce point de vue, j'insisterais sur un point qui est très important. Etant donné l'interconnexion générale des acteurs, phénomène qui ne cesse d'évoluer au gré des évolutions technologiques du marché, il est difficile de définir des limites à ce que l'on doit protéger. Donc, face à une attaque massive d'un type que nous n'avons pas encore complètement vécu mais qui n'est pas improbable, il faut vraiment réfléchir de manière systémique sur ce qui peut être attaqué et ce qui peut poser des problèmes. Pour la souveraineté nationale, que constatons-nous maintenant ? Le premier constat est que les attaques ne cessent d'évoluer en complexité, en ciblage et en effet. Parallèlement, les systèmes de défense qui existent et qui sont encore très largement influencés par une notion de défense périmétrique ne suivent pas et donc il y a un risque aujourd'hui de décrochage entre les menaces d'une part, et les défenses d'autre part. les menaces ne concernent pas que les systèmes d'information traditionnels. Elles peuvent aussi s'adresser aux réseaux industriels et provoquer des actes de sabotages qui sont une vraie question aujourd'hui ouverte. On s'aperçoit que face à un champ d'effet considérable sur le plan de la menace, le niveau actuel de défense des entreprises est insuffisant.
Nous ne somme pas les seuls à le dire et c'est une prise de conscience qui apparaît. Il n'y a rien de choquant en soi, mais il faut être conscient que nous sommes dans un domaine extraordinairement dynamique où d'une part les attaquants font preuve d'une très grande ingéniosité et, d'autre part, le champ d'attaque ne cesse d'évoluer avec l'introduction des smartphones, la notion de « *bring your own*

device », le fait de l'utilisation croissante dans l'entreprise de nos propres outils sans toutes les précautions utiles. La découverte que tous les systèmes, y compris les systèmes sensibles, ont une part d'interconnexion conduit à penser complètement différemment.

Jean-Claude BOURRET

J'ai une deuxième question à vous poser : puisque vous vendez en quelque sorte de la protection aussi bien pour des industries privées que pour la défense nationale, comment faites-vous pour tester la fragilité éventuelle d'un système de protection ? Ma question est évidemment à tiroirs, parce que, si vous testez les barrières de sécurité qui protègent un système ou des données, vous êtes obligés d'utiliser des hackers identifiés. Peut-on imaginer, comme on l'a révélé pour certains fabricants de systèmes de protection privés, d'antivirus etc… qu'ils ont rémunéré des gens qui réalisent des attaques pour qu'ensuite ils puissent voir l'entreprise ou le ministère en question en leur disant « *vous voyez, vous avez été pénétré par des hackers, il est temps que vous achetiez mon produit !*».

Stéphane JANICHEWSKI

Oui, il est bien sûr possible de tester ou faire des tests de pénétration. D'ailleurs, c'est fait très régulièrement. Je dirais que la question n'est pas tellement dans le fait de savoir s'il y a eu pénétration ou pas pénétration.
Aujourd'hui, étant donnée l'évolution de la menace, on sait que nous sommes dans un domaine de risques et qu'il faut avoir une approche par rapport au risque, la question en matiere de protection à laquelle vous pouvez répondre est d'essayer de réduire le risque au minimum, sachant que le risque zéro n'existe pas dans ce domaine. Sous un premier aspect, on doit faire en sorte que pour l'attaquant, la barrière à franchir soit de plus en plus élevée.
Deuxième aspect; la question n'est pas d'éviter une attaque extraordinairement sophistiquée et préparée mais d'en limiter les conséquences. Ce qui est important, par des systèmes beaucoup plus pro-actifs, est d'identifier les indices d'attaques et d'en limiter les conséquences. Il faut donc être capable de pouvoir intervenir le plus vite possible pour faire en sorte que cette attaque soit connue et que les effets de propagation au sein de l'entreprise ou au sein de l'organisme public soient limités également. C'est la question aujourd'hui, celle d'une défense beaucoup plus systémique, beaucoup plus dynamique, beaucoup plus en profondeur et qui suppose au passage, non seulement des dispositifs techniques mais surtout la mobilisation de tous les acteurs au sein de l'organisme. C'est une notion clé, chaque acteur est potentiellement une source de menace par négligence ou éventuellement par malveillance. Il faut surtout bien former, bien sensibiliser un acteur de la défense et chacun doit participer au considérable relèvement du seuil d'attaque nécessaire.

Jean-Claude BOURRET

On a vu récemment des vols de données, un stagiaire avec une simple clé USB peut voler des données extrêmement sensibles. Je me pose une question extrêmement simple : est-ce qu'il y a des systèmes qui permettent de verrouiller cela ? Faut il supprimer les ports USB ? faut-il mettre en place un système de cryptage ou de traçage qui permet de voir que l'on a extrait des données ou qu'on les a copié

sur une clé USB ? Comment faites-vous ?

Stéphane JANICHEWSKI

Oui, il y a des outils mais il y a surtout des questions d'organisation. Vous évoquez en fait la question des données. La première chose à faire, avant même d'envisager la combinaison, l'organisation et des outils, est d'engager une réflexion sur la définition des données sensibles ? On va éviter de donner à un une stagiaire un accès libre sur des données sensibles. Les données sensibles doivent rester difficiles d'accès. A partir de là, on peut construire un ensemble de mesures qui vont permettre de limiter le risque à un niveau acceptable. C'est une construction à partir d'une vraie réflexion de fond qui intègre une prise de conscience nécessaire au niveau des entreprises quant au fait que l'information est de plus en plus un « *actif* » absolument essentiel.
En d'autres termes, tout ce qui tourne autour du système d'information n'est pas simplement de l'ordre de l'intendance et une source de coût qu'il faut réduire en permanence mais une dimension stratégique pour l'entreprise qui peut être génératrice d'efficacité sous réserve de régler les problèmes de sécurité.
L'actif formé par les données revêt une grande variété. Des données sont stratégiques pour l'entreprise: tout ce qui tourne autour de la propriété intellectuelle et ce qui va permettre de faire tourner la production, par exemple. Les données qui sont confiées par les clients sont extrêmement sensibles ainsi que celles qui touchent au domaine des ressources humaines. Il faut réfléchir à la manière de les gérer de manière intelligente et utiliser des outils dédiés. Vous comprendrez, par rapport à ma réponse, que la question n'est pas tellement dans les outils. On a un peu trop tendance à se tourner vers la technique en se disant qu'elle va résoudre les questions. La technique ne résoudra pas les questions qui n'ont pas été clairement posées au sein de l'organisme.

Jean-Claude BOURRET

Une dernière question si vous le voulez bien : vous pensez que les sociétés privées en France, les PMI, les PME et même un peu au-delà, ont conscience de la richesse de leur savoir-faire et de la nécessité de le protéger ?

Stéphane JANICHEWSKI

Malheureusement, force est de constater, que la prise de conscience, même si elle évolue positivement, reste quand même insuffisante. il est quand même navrant de voir que certaines entreprises sont pillées, en termes d'espionnage industriel, par manque de prise de conscience, par le fait que l'on n' a pas considéré que c'était un enjeu suffisamment important.
Le côté positif, c'est que les choses commencent à évoluer et, je crois que, de ce point de vue, l'action publique qui a été conduite depuis un certain nombre d'années commence à porter ses fruits. Je crois que cette préoccupation commence à monter dans les strates de responsabilités des entreprises, parfois avant même qu'il y ait eu une attaque importante. Il n'empêche que sur les années récentes, trop d'attaques ont eu lieu qui ont affecté nos entreprises stratégiques.

Jean-Claude BOURRET

Peut-on peut avoir une idée du temps qu'il faut à vos spécialistes pour évaluer le niveau de sécurité d'une entreprise voire d'un organisme

public et quelle est la fourchette des investissements nécessaires pour assurer cette sécurité ?

Stéphane JANICHEWSKI

C'est un petit peu difficile de répondre parce que cela dépend du nombre de personnes à interroger notamment celles qui sont dans des postes « *clé* ». Pour les raisons que j'indiquais tout à l'heure, on ne peut pas se contenter d'interviewer le responsable de la sécurité ou le directeur des systèmes d'information parce que la problématique va toucher en fait tous les directeurs c'est-à-dire les directeurs opérationnels, les directeurs métier, tous ceux qui sont amenés à utiliser des données. Une approche par le risque donc centré sur les données suppose d'interroger suffisamment de personnes et de détecter le « *maillon faible* » qui détermine le niveau de protection. Il faut aller identifier de manière assez globale là où il n'y a « *rien* », là où il y a des interconnexions, là où il y aurait des points de vulnérabilités au regard de la politique de sécurité tout en s'assurant de son application. On peut faire une évaluation assez rapide en quelques semaines fondée sur l'analyse de risque, c'est ce que l'on préconise, et de quelques semaines à quelques mois pour une analyse beaucoup plus importante.

Jean-Claude BOURRET

Et aucune indication de prix ?

Stéphane JANICHEWSKI

On évalue entre 10 à 20% du coût de l'opération des systèmes d'information ce qu'il faut affecter à la sécurité. Cela n'est pas négligeable mais pas hors d'atteinte au vu des enjeux.

Jean-Claude BOURRET

Merci monsieur JANICHEWSKI pour cette intervention qui nous permet de mieux cerner les problématiques de ce domaine. Je vais maintenant donner la parole au général Éric BONNEMAISON. Vous êtes directeur adjoint de la Délégation aux affaires stratégiques. Vous assistez le ministre de la Défense en matière de politique de défense et de relations internationales. La délégation aux affaires stratégiques contribue également à la réflexion stratégique et prospective du ministère. Au quotidien, la DAS participe activement à la définition des positions de défense à l'OTAN, à l'Union européenne notamment en matière de cyberdéfense. Vous avez commandé les écoles de Saint-Cyr Coëquidan et vous avez lancé en 2012 avec monsieur SALVADOR, la chaire de cyberdéfense-cybersécurité entre les écoles de Saint-Cyr Coëtquidan, SOGETI et THALES.
Qu'entendez-vous lorsque vous parlez du cyberspace en tant qu'espace duel ? Souvent en effet, faire la distinction entre civil et combattant, entre système militaire et infrastructure civile, entre attaque et délit ? Quel est le point de vue militaire ?

Général Éric BONNEMAISON

Ce forum doit permettre de mieux comprendre la réalité de la cybersécurité aujourd'hui. Je crois que le ministère de la défense s'inscrit totalement dans cette démarche, comme le montre le nombre de militaires présents dans cette salle. Le concept de continuum, comme tous les concepts, pourrait être discuté à loisir entre spécialistes mais ce serait peu opérant et peu clair pour ceux qui nous écoutent. Je vais plutôt donner la perception qu'a le ministère de la

défense de ce rapprochement entre cybersécurité et défense.
C'est une idée assez ancienne. On pourrait remonter au début du XXème siècle avec l'instauration de l'ancêtre du SGDSN qui assurait déjà une coordination civilo-militaire de la défense nationale. Vous vous souvenez que l'ordonnance de 1959 a donné une définition assez large de la défense nationale puisqu'elle a été qualifiée de globale. Elle regroupait la défense armée, la défense civile qui était chargée de la défense de la population, de l'ordre public et des institutions mais il y avait aussi la défense économique, la défense culturelle qui avait pour but de maintenir, de préserver l'esprit civique et les valeurs républicaines.
Le Livre Blanc de 2008 a fait émerger ce qui a été qualifié de « *stratégie de sécurité nationale* » qui était assez novatrice parce qu'elle visait finalement à mettre en cohérence les différentes politiques publiques, dont la politique de défense, au service du concept de résilience de la nation que vous connaissez tous, donc résilience de la nation des pouvoirs publics mais aussi de ses intérêts à long terme.
Parfois les différences entre sécurité et défense peuvent ne pas être très claires. Tout le monde voit bien à quel registre appartient la police de la route d'un côté et la dissuasion nucléaire de l'autre. Vous voyez bien que les concepts sont très différents mais parfois la frontière est plus floue et c'est typiquement le cas en ce qui concerne le cyber. Je vais essayer de montrer ceci : plus encore que dans les autres domaines typiquement militaires pour les forces armées, le cyber représente pour la défense un défi stratégique qui doit être pensé dans un cadre plus englobant que les strictes opérations militaires. Il doit recouvrir les domaines par exemple juridiques, technologiques, mais aussi les relations internationales. Je vais développer tout cela.
Je dirais d'abord que le cyber introduit pour les armées une nouvelle vulnérabilité. Je dois dire que les systèmes de commande et de contrôle aujourd'hui vont jusqu'au plus bas échelon de la hiérarchie. Vous connaissez les systèmes tout en haut et peut-être que Patrick PAILLOUX en parlera mais je voudrais donner l'exemple du système FELIN qui équipe aujourd'hui le combattant du futur, en fait qui est le combattant actuel et qui inclut des systèmes informatiques. Il nécessite des réseaux haut débit en métropole et sur chaque théâtre d'opération. Il nécessite aussi de puissants systèmes de traitement de l'information. Or, il faut bien admettre que les forces armées utilisent des versions plus ou moins améliorées des systèmes que l'on peut trouver dans le secteur civil et que nous avons tous sur nos ordinateurs. Les protocoles sont basés sur l'IP, les postes de travail utilisent donc massivement des PC avec des logiciels qui sont grand public. Bien sûr les systèmes les plus critiques, je pense par exemple à la dissuasion nucléaire, ont des systèmes spécifiquement protégés. Mais la défense peut être victime de toutes ces attaques qui ne sont pas forcement ciblées et qui arrivent par internet et qui peuvent affecter la périphérie des systèmes de défense, voire plus.
Je voudrais citer, par exemple, le cas typique du virus Conficker en 2008 : il a été transféré via internet, depuis une clé USB, sur les systèmes de défense et il a obligé d'arrêter le réseau pour le dépolluer. Il a affecté un certain nombre de domaines.
A côté de ce que je pourrais appeler le « *bruit de fond cyber* », on a bien entendu des attaques spécifiquement ciblées sur les armées : ce sont par exemple des activités d'espionnage, de tentative de paralysie voire de des-

truction de systèmes informatiques. Le problème se pose avec acuité non seulement pour les systèmes de commandement mais aussi pour les systèmes d'armes. Toutes les plateformes de combat, que ce soient les bateaux, les avions embarquent massivement à bord des systèmes informatiques et électroniques. Certains systèmes sont spécifiques, par exemple le radar à balayage électronique, mais beaucoup comportent des équipements achetés sur étagères. D'autres sont quasiment identiques à ce que l'on trouve dans le civil. Par exemple, quelle différence y a-t-il entre une chaufferie EDF et une chaufferie d'un sous-marin nucléaire ? Quelle différence entre le SCADA qui pilote sur des frégates et un SCADA utilisé dans les industries ? Je dirais que malheureusement, il n'y a pas assez de différences. La force des forces armées aujourd'hui, c'est leur technologie, entre autres, mais elle est devenue une vulnérabilité. La cyberdéfense militaire s'intéresse donc à l'ensemble des systèmes qui sont utilisés depuis leur conception, leur réalisation, leur fabrication, leur exploitation opérationnelle mais aussi leur maintenance. Tout ces systèmes sont fortement dépendants des technologies et de prestataires civils, voire d'étrangers. Quelle serait la crédibilité d'une dissuasion qui comporterait des composants qui ne sont pas maîtrisés et qui viennent de l'étranger ?

Le cyber est aussi devenu un domaine stratégique où l'asymétrie est reine. Il s'agit d'abord de peser sur la volonté d'adversaires et le cyber, dans ce cas là, se révèle un moyen de choix. Il permet, par exemple, d'influencer directement la population civile grâce à Internet. Il permet de paralyser ou de désorganiser les secteurs clés dans des proportions qui sont finalement ajustables. Cela peut aller de la simple gêne à un déni de service par exemple. Cela peut aller jusqu'à la désorganisation brutale et durable de la société en frappant des infrastructures vitales. Les états peuvent aussi décider d'avancer masqués, ce qui est plus facile dans le cyberespace - parce qu'on ne voit rien - que dans le domaine du monde conventionnel. Et cela laisse la place à toutes les manipulations imaginables : par exemple, le cyber en frappant les sites civils par des moyens relativement stratégiques qui intéressent tous les états. Les états les moins avancés sont du reste les moins vulnérables aux cyberattaques et les plus intéressés par ce moyen d'un relatif faible coût. Une clé USB infectée peut faire plus de dégâts à un centre de commandement et de contrôle qu'une bombe de 250kg à précision métrique. J'utilise toujours l'analogie suivante : un hacker, tout seul chez lui, avec un simple ordinateur possède la puissance de feu d'une kalachnikov, à cette différence que son ordinateur peut tirer à des milliers de kilomètres, instantanément.

Ce pouvoir égalisateur du cyber permet ainsi au faible de frapper le fort là où il est faible et d'éviter de se confronter à lui sur un terrain conventionnel avec des armes classiques. Les états les plus puissants peuvent également trouver dans le cyber, un outil de basse intensité qui leur permet de compléter le spectre des effets des autres armes conventionnelles dont ils disposent. Le cyber est surtout le moyen de lutte idéal pour des groupes non étatiques. Ces derniers peuvent affronter à distance un état avec finalement un rapport coût/efficacité qui est particulièrement avantageux pour eux. Pire encore ! tout l'ordre international qui fixe les frontières et les rapports entre les états est alors à leur avantage puisqu'il gêne les poursuites en multipliant les obstacles juridiques et politiques qui sont loin d'être résolus et sur lesquels travaille la communauté internationale

dans le domaine juridique. Finalement, aujourd'hui, chaque individu peut se servir du cyberespace pour servir une cause et éventuellement porter atteinte à un état, que ce soit le sien ou un autre.
On a vu par exemple le glissement d'Anonymous : en défendant la liberté d'internet, il s'est attaqué à des états qui luttaient contre la censure ou qui pratiquaient la censure. Il a aussi assumé son engagement contre Israël pour des raisons politiques. On le voit aujourd'hui au Mali, la France n'est pas épargnée par des attaques informatiques liées à son engagement. Donc, le concept westphalien des relations internationales déjà battu en brèche par le terrorisme international, est remis en cause par le cyber. Avec cet outil, n'importe quel groupe déterminé peut contester la politique d'un état et tenter de lui faire changer d'avis sous peine, finalement, de porter atteinte gravement à son fonctionnement.
Du point de vue du ministère de la défense, il y a un certain nombre de conséquences avec la multiplication des agresseurs potentiels. Le premier problème est d'arriver à faire le tri de toutes ces attaques, différencier celles qui relèvent de la cybercriminalité et celles qui portent atteintes aux capacités des forces armées et aux intérêts vitaux de la Nation. Les malwares divers, les défaçages, les spams génèrent un bruit de fond cyber qui occupe inutilement nos spécialistes et rendent plus difficile la détection des vraies attaques ciblées et dangereuses.
Une coopération étroite est déjà lancée avec l'ANSSI. Elle est nécessaire pour mieux classifier la menace et choisir la réponse la mieux appropriée. Est-ce que l'on applique un traitement judiciaire, diplomatique ou d'un ordre politique ? La défense profite de tous ces efforts qui sont faits pour faire baisser la criminalité. Chaque mois, il y a des citoyens tentés ou des outils qui sont disponibles en ligne. On arrivera à dissuader ces attaques en complétant cet arsenal par une politique pénale.
La défense est aussi intéressée par la diminution des menaces qui pèsent sur les infrastructures critiques. Les attaques sur ces systèmes fragiliseraient la société, obligeraient probablement les forces armées à intervenir auprès des populations et obèreraient une partie des capacités militaires. Elles pourraient déboucher sur une escalade stratégique. Après tout, les Etats-Unis ont déjà annoncé qu'ils n'hésiteraient pas à riposter par tout moyen, y compris conventionnel, à une attaque cyber contre leurs intérêts vitaux. On voit bien l'importance et le continuum qu'il y a entre une menace cyber et une attaque matérielle conventionnelle.
En France, la doctrine n'est pas aussi clairement établie, mais le Président de la République dispose finalement de toute son autorité pour apprécier la réponse qui serait adaptée dans un tel cas.
Au niveau national beaucoup été fait, que ce soit au ministère de l'intérieur ou au ministère de la défense et je pense que le Livre Blanc proposera un certain nombre de pistes. En revanche, au niveau international, il reste encore beaucoup à faire. Je ne vais pas dire que rien n'a été fait, mais il reste beaucoup à faire.
La Convention de Budapest, ratifiée par la France, impose à une trentaine d'états-partie de coopérer dans la lutte contre la cybercriminalité. Cela n'engage malheureusement que les signataires qui sont d'ailleurs tous des états occidentaux et finalement ça ne repose que sur la bonne volonté. Les conceptions très différentes des états ne facilitent pas les choses. La définition d'un terroriste diffère sensiblement que l'on soit à Washington, Paris, Moscou ou

Pékin. Alors quand l'on cumule le cyber et le terrorisme, vous voyez bien l'enjeu. Tous les états conviennent qu'un manque de contrôle donne des opportunités relatives à la cybercriminalité pour les groupes non étatiques. Pourtant un certain nombre d'états n'ont pas encore introduit dans leur législation des cyberinfractions. D'autres ne le peuvent pas et ne sont pas en mesure de les poursuivre par manque de moyen et enfin le reste n'en veut absolument pas parce que, finalement, ça sert leurs intérêts.

Pour mémoire, comme l'a rappelé le général WATIN-AUGOUARD, vous vous souvenez des attaques contre l'Estonie en 2007 qui avaient une vraie dimension stratégique et avaient finalement bloqué toute une société en signe de désaccord politique. Au final, la Russie n'a condamné qu'un seul étudiant à une peine symbolique.

Tous les États conviennent également, qu'il faut faire entrer le cyber dans le cadre classique des relations internationales sous peine d'augmenter dramatiquement les comportements conflictuels. Le cyber révolutionne en effet le jus ad bellum, c'est-à-dire le droit qui détermine si on est en guerre ou non. je vais vous poser quelques questions simples auxquelles il est compliqué de répondre : quelle attaque cyber peut être considérée comme une attaque armée ? Faut-il des morts ou des destructions physiques pour donner le droit à la légitime défense prévue à l'article 51 de la Charte des Nations unies ? Autres questions : est-ce qu'une paralysie de service essentiel à une nation est suffisante ? Au-delà des conséquences, comment s'assurer de l'identité de l'agresseur ? Et on connaît tous la problématique de l'imputabilité. Est-ce que le temps de mener l'enquête par des moyens techniques ou de renseignement, ne laisse pas une fenêtre de vulnérabilité encore plus importante qui donne une vraie prime à l'agresseur ?

Et puis je vais parler du droit dans la guerre, le jus in bello : qu'est-ce qu'une attaque proportionnée ? Comment d'ailleurs évaluer les dommages subis ou les dommages infligés ? Autres questions : qu'est-ce qu'un dommage collatéral quand tous les systèmes sont interconnectés et peuvent servir à une attaque cyber ? Qu'est-ce que le respect des états neutres quand le réseau mondial est interconnecté ? Qu'est-ce qu'un combattant ou un non-combattant à l'heure du cyber ? quand n'importe qui peut à partir de chez lui, participer à une attaque cyber sur un pays ? Est-ce que la mère de famille ou le retraité qui s'impliquent dans un conflit étranger on l'a vu en Syrie, au Liban, en Libye qui lèvent des fonds, qui diffusent de faux renseignements ou des renseignements classifiés, qui lance des attaques en déni de service, sont des cibles légitimes des états qui ont été attaqués ? Est-ce qu'ils pourraient être poursuivis si leurs actions participent aussi à des crimes de guerre ?

Donc, vous voyez bien que le cyber est l'illustration du continuum cybersécurité et défense : que ce soit de l'acte criminel aux opérations stratégiques, de la gêne à la destruction de l'État au simple individu, le cyber embrasse tout le spectre des nations, des intentions, des conséquences. Il exige donc une réponse qui couvre tout le spectre et qui nécessite - ça été dit tout à l'heure - la mobilisation et la collaboration de tous les acteurs de la société. Je crois que pour la France, la défense y prend sa place, elle n'est pas hégémonique, et elle doit assumer son rôle particulier lié notamment aux opérations.

Jean-Claude BOURRET

Merci beaucoup mon général. Et bien, le plus difficile n'est pas de résoudre les problèmes, c'est de bien poser les questions. Mon général vous avez bien posé les questions et je vais vous en poser une autre : comment se fait-il que le ministère de la défense ne centralise pas l'ensemble de la cybersécurité ?

Général Éric BONNEMAISON

La réponse est simple, c'est que le gouvernement a demandé que ce soit la responsabilité de l'ANSSI qui est finalement l'autorité nationale de cyberdéfense. La Défense, elle, est responsable de ses propres systèmes, que ce soit en France, en opération ou sur ses équipements et je crois qu'elle peut largement coopérer avec l'ANSSI et aider lorsqu'il s'agit de défense ou d'attaques cyber qui se déroulent soit en France, soit sur nos équipements, soit éventuellement en opération.

Jean-Claude BOURRET

Que pensez-vous éventuellement de la proposition de la Chine et de la Russie d'établir un nouveau traité sur la cybersécurité mondiale ?

Général Éric BONNEMAISON

Comme je l'ai dit tout à l'heure, un certain nombre d'enceintes travaillent sur la question de la cybersécurité. Le Conseil de l'Europe a produit la Convention de Budapest qui est centrée sur la lutte contre la cybercriminalité.
L'ONU planche aussi sur ce domaine là, sur un texte qui est plus orienté « *relations internationales* ». La Russie et la Chine ont proposé un Code de bonne conduite dans le cadre de l'organisation de sécurité de Shanghai mais ce texte va finalement à l'encontre des intérêts de la France et d'un certain nombre de pays européens et ce pour deux raisons. La première c'est qu'il insiste d'abord sur la sécurité de l'information, alors que nous insistons plus sur la sécurité des réseaux. Le texte pourrait donc aboutir à une censure du contenu d'internet. La deuxième raison, c'est qu'actuellement une campagne de propagande peut être considérée par ces états comme une agression qui vise à déstabiliser un régime politique. Pour nous, ceci va à l'encontre de la liberté d'expression et peut être finalement une extension des causes de conflictualité.

Jean-Claude BOURRET

Merci mon général. Nous allons continuer à feuilleter le grand livre de la cybersécurité avec monsieur Patrick PAILLOUX qui est directeur général de l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information. Monsieur PAILLOUX, comment faire face aux menaces ? Et que fait l'état ?

Patrick PAILLOUX

Que fait l'état ou que peut faire l'état ? Tout d'abord, par rapport à quoi ? Quelle est la menace contre la sécurité nationale telle que nous l'analysons, telle que nous la voyons tous les jours ? Je ne vais pas vous parler de science-fiction, mais je vais vous parler de ce que l'on mesure concrètement tous les jours. La première particularité, c'est que la menace à laquelle nous sommes confrontés est très asymétrique, au sens où les acteurs qui menacent la nation peuvent être de toute nature, depuis des individus jusqu'à des états, en passant par une hybridation de la grande criminalité qui

s'intéresse de plus en plus au domaine cyber. Cette menace est évidemment très internationale puisque, dans ce domaine, les frontières n'existent pas. Pire, les frontières sont un carcan pour les défenseurs comme nous et plutôt un avantage pour les attaquants. Cette menace est très présente notamment en matière de cyberespionnage. Malheureusement, j'ai déjà eu plusieurs fois l'occasion de le dire, on ne compte plus les très grandes entreprises qui sont victimes de pillage technologique au travers de l'espionnage informatique. Ce n'est malheureusement pas une menace théorique mais bien une réalité aujourd'hui. Cette menace est en perpétuelle évolution. Pour ceux qui suivent le domaine, il ne se passe pas un jour ou une semaine sans qu'apparaissent de nouvelles vulnérabilités, de nouveaux modes d'attaques. Et enfin, nos sociétés sont extrêmement fragiles. Il n'existe aucun domaine de la vie courante qui ne dépende aujourd'hui de l'informatique ou des télécoms, que ce soit dans le domaine de la santé, de la finance, du transport, de la production et de la distribution d'énergie, de l'alimentation. Ce sont autant de points de fragilité qui peuvent être exploités par nos ennemis, les ennemis de la France ou de nos alliés. Nous sommes dans une situation où les acteurs qui vont s'intéresser à ces vulnérabilités ne sont pas forcément bien intentionnés, et où un certain nombre d'entre eux travaillent aujourd'hui, on le voit, à la réalisation d'attaques informatiques contre les infrastructures critiques. Il y a déjà quelques exemples d'attaques contre des infrastructures à l'étranger et je suis sûr qu'ils seront évoqués au cours de ces deux journées. Notre capacité à gérer et à protéger nos infrastructures sera sans doute un des points évoqués dans le prochain Livre Blanc de la défense et de la sécurité nationale. Face à cette situation, qui finalement s'est significativement dégradée depuis le Livre Blanc de 2008, l'état ne peut bien sûr pas rester inactif, et il ne l'est d'ailleurs pas. Un des bras armés de l'état dans ce domaine, c'est l'ANSSI, sous l'autorité du Premier ministre, dont la mission est d'organiser la défense du pays. Même si bien d'autres acteurs interviennent : le ministère de l'intérieur, le ministère de la défense, le ministère en charge de l'économie numérique. Ils sont très présents dans la salle, y compris au plus haut niveau, et ils auront l'occasion de détailler largement leur action.

J'en profite pour répondre à la question de tout à l'heure : est-ce qu'il y a des personnes au top de la technique ? Oui, il y en a, le problème n'est pas uniquement de savoir s'il y a des gens de bon niveau en France. Oui, il y en a beaucoup au ministère de la défense, au ministère de l'intérieur et encore plus à l'ANSSI, mais ce n'est pas suffisant.

Depuis le dernier Livre Blanc sur la défense et la sécurité nationale de 2008, qui a pour la première fois érigé cette question comme une menace stratégique, beaucoup a été fait et dans deux domaines : d'une part la prévention, d'autre part notre capacité à réagir et à agir en cas d'attaques contre des infrastructures critiques. Vous connaissez sans doute, j'ai eu plusieurs fois l'occasion d'en parler, notre capacité à intervenir lors d'un certain nombre d'attaques, à agir en cas d'attaques informatiques et notre rôle d'assistance notamment auprès des très grandes entreprises qui sont victimes d'attaques informatiques, notre rôle pour protéger l'État etc…

Mais c'est d'autre chose dont je veux vous parler aujourd'hui, pour être un peu concret. L'état et l'ANSSI peuvent sans doute beaucoup, mais ne peuvent pas tout faire et ne pourront jamais tout assumer seuls. Pour oser une ana-

logie, qui certes à ses limites, on a bien une police et une gendarmerie pour nous protéger, il n'empêche que lorsque vous sortez de chez vous, vous fermez probablement votre porte d'entrée à clef. Et certains d'entre vous, surtout les professionnels, il y en a beaucoup dans cette salle, utilisent sans doute des entreprises de surveillance et de gardiennage. Je veux dire par là que chacun doit assumer sa part de travail, notamment en ne laissant pas les portes ouvertes.

Le rôle de l'état dans ce domaine est de mettre en place les conditions permettant à chacun de se protéger. Il y a évidemment un important rôle de sensibilisation et de formation et c'est sur ces deux points que je souhaite insister aujourd'hui.

Ceux qui suivent un peu notre domaine savent qu'au mois d'octobre 2012, l'ANSSI a publié, pour appel à commentaires, un guide d'hygiène informatique. Ce guide se veut être l'alpha et l'oméga de la sécurité des systèmes d'information. Autrement dit, ne pas appliquer les règles de ce guide revient à sortir de sa voiture en laissant les clefs sur le tableau de bord ou sur le contact. J'en profite pour signaler, en utilisant cette analogie, que si vous faites ça, votre compagnie d'assurance ne vous remboursera sans doute pas. Il y a sûrement dans notre domaine un point à creuser en utilisant cette analogie.

On a essayé de prendre en compte ces remarques, mesure par mesure, il y en a 40. On les a un peu modifiées, mais on est resté sur le nombre. Au premier type de remarques, celles qui nous disent que nous n'avons rien inventé, je veux répondre que c'est vrai. Il n'y a aucune nouveauté dans ces mesures mais ce guide ne s'adresse pas qu'aux experts de la sécurité. Malheureusement, ce que l'on constate c'est que généralement ces règles ne sont pas appliquées, et que des mesures de sécurité beaucoup plus sophistiquées ne serviraient à rien si ces règles élémentaires ne sont pas mises en œuvre.

Au second type de remarques, celles qui nous disent que nous n'avons rien compris au fonctionnement d'une entreprise, je vais répondre « *si* ». Nous connaissons le terrain et nous le connaissons de mieux en mieux notamment parce que nous vous accompagnons. Nous intervenons très souvent au sein des administrations, au sein des entreprises à la fois à l'occasion d'attaques informatiques, et pour aider à mettre en place des systèmes d'information qui nécessitent un haut niveau de sécurité. Et c'est bien face à ce constat que nous faisons quand nous intervenons que nous sommes convaincus qu'il faut changer les comportements. Et vous verrez que dans le document définitif nous avons essayé d'être le plus pédagogique possible. Nous savons, vous nous l'avez dit, que certaines des mesures sont beaucoup plus complexes que d'autres à mettre en œuvre, et nous avons essayé d'expliquer que pour telle mesure, il fallait commencer par telle action. Et que si cette action était trop difficile, il y avait sans doute une première étape à franchir. Et que si cette première étape était encore trop difficile, il y avait sûrement une sous-étape qui pouvait être à franchir. Donc on a essayé

« Le rôle de l'état dans ce domaine est de mettre en place les conditions permettant à chacun de se protéger. »

d'être le plus pédagogique possible, et je suis très heureux de vous annoncer aujourd'hui, officiellement, la publication du guide définitif. J'imagine qu'il évoluera, car j'espère bien que vous continuerez à nous faire des remarques. Vous avez ici le premier guide officiel de l'ANSSI en matière d'hygiène informatique qui bien sûr, comme l'ensemble des documents que nous publions, est librement téléchargeable. Vous pourrez le voir sur notre stand que je vous invite à visiter. Vous pouvez l'utiliser, le réutiliser, il est d'utilisation libre et on souhaite qu'un maximum de personnes l'utilisent.

Je répète ce que je disais en octobre, et je pense que je le répéterai encore et encore et encore, descendre en-dessous de ces recommandations est probablement inacceptable pour quelqu'un qui a des données à sécuriser.

Ces 40 règles, je souhaite aussi qu'elles soient enseignées dans les écoles d'informatique, dans les écoles d'ingénieur et dans les universités. Il n'y a rien de pire que de voir des jeunes sortir d'écoles, d'écoles d'ingénieur, d'universités, d'IUT, auxquels on n'a pas enseigné ces rudiments de la sécurité et ces bonnes pratiques en matière de sécurité. Il ne s'agit pas d'enseigner l'alpha et l'oméga des règles de crypto mais juste ces règles élémentaires. Sans cette base élémentaire, c'est finalement assez logique que sur le terrain, quand ces personnes viennent ensuite travailler dans les entreprises, dans les SS2I, que ce qu'elles font ne soit pas compatible avec des règles élémentaires de sécurité. Donc je souhaite très ardemment que ces règles soient aujourd'hui enseignées.

La formation, c'est le deuxième sujet que je souhaitais rapidement évoquer devant vous. On ne forme pas assez d'experts, de spécialistes ou de généralistes en matière de sécurité informatique. J'en recrute beaucoup et on me le reproche d'ailleurs régulièrement d'aspirer trop largement les experts. De fait, on n'en forme pas assez, probablement le quart de ce qu'il faudrait. Donc, nous nous sommes attelés à la tâche de rédiger un référentiel de formation qui ne vise pas les experts techniques ultra-pointus sur tels et tels sujets de la cybersécurité, mais ce que nous avons appelé des architectes référents. Derrière ce jargon se cachent tous ceux qui, dans une entreprise ou une administration, sont à la manœuvre en matière de sécurité des systèmes d'information. Ce sont les personnes vers lesquelles les informaticiens se tournent quand ils ont une question, ce sont ceux qui comprennent le fond des choses, qui sont capables d'en décortiquer les détails, autrement dit, ce sont des gens à qui « *on ne le fait pas* » en matière de sécurité informatique, ce sont ceux qui sont capables de réagir quand il y a un incident informatique, de bâtir une architecture sécurisée, de dérouler une démarche d'homologation.

Ce référentiel décrit l'ensemble des compétences et des savoir-faire nécessaires. Ce référentiel s'adresse aux écoles, aux universités, pour adapter si nécessaire leur cursus de formation, le créer éventuellement. Il s'adresse évidemment aux centres de formation professionnelle, aux centres de formation continue, mais il s'adresse aussi aux directions des ressources humaines ou aux services informatiques pour recruter les bonnes personnes et définir les cycles de formation adaptés. Enfin, naturellement il s'adresse à nous tous, à notre communauté, aux gens qui travaillent dans le domaine pour qu'ils puissent eux-mêmes se positionner sur ce référentiel, vérifier leurs compétences et se former s'ils ont une faiblesse dans un domaine, acquérir les compétences qui leur manque.

Ce référentiel est lui aussi publié aujourd'hui, disponible gratuitement, sur notre stand, téléchargeable. Utilisez-le!
Vous l'avez compris, la volonté de l'état, de l'ANSSI, c'est de vous donner toute la documentation possible, technique, méthodologique, pour tous les acteurs de la sécurité, les décideurs, les DRH, pour que les choses changent.
En l'espace d'un an, je n'ai pas compté le nombre de recommandations, de guides que nous avons publiés, des guides techniques, méthodologiques, vous pouvez retrouver tous ces éléments à la fois sur notre site internet et sur notre stand, n'hésitez pas à les utiliser.
Mon discours sur ce point n'a pas bougé d'un millimètre depuis quelques années, la sécurité informatique c'est du concret, les attaques informatiques sont une réalité et pas de la science-fiction. Sécuriser un système d'information ce n'est pas impossible, cela repose sur l'application de règles techniques, de comportements pas si difficiles à mettre en œuvre. Cela nécessite aussi de faire appel à des prestataires, à des experts et à des professionnels du métier. Ils sont nombreux à ce forum, et c'est la dernière chose que je voulais faire, les saluer aujourd'hui, les remercier d'être présents. En ce qui nous concerne, nous essayons de les aider dans la mesure de nos moyens mais surtout, le meilleur moyen de vous aider, c'est de vous inciter à faire appel à eux. Ce sont des professionnels qui peuvent vous aider à sécuriser vos propres infrastructures.

Jean-Claude BOURRET

Merci infiniment monsieur PAILLOUX, je me posais une question en vous écoutant et en découvrant que l'on pouvait télécharger sur le web votre fascicule avec 40 points. Je me demandais si un hacker facétieux ne pouvait pas pirater guide en en modifiant les recomandations…

Patrick PAILLOUX

Ça serait un hacker facétieux comme vous dites mais non, ce qu'on espère c'est que notre guide soit viral et qu'on le retrouve partout, tout comme certaines données qui se retrouvent partout sur internet alors qu'on ne voulait pas qu'elles soient publiées ! Plus sérieusement, depuis quinze jours, je l'ai relu plusieurs fois pour vérifier si ce que l'on disait avait du sens. Ce sont en fait des règles élémentaires. Il me semble donc compliqué, pour les gens compétents, de les modifier en ajoutant des règles qui seraient contraires à la sécurité.
L'objectif de ce guide ce n'est pas de définir des règles qui auraient été inventées par l'ANSSI. On ne dit pas « *si vous faites ça, vous serez sécurisés* ». Mais il est bon d'avoir un ensemble d'éléments, un ensemble de règles, pour que ces règles soient enseignées, pour que les gens les connaissent et qu'elles soient appliquées partout. C'est n'est pas quelque chose qu'on a sorti de notre chapeau, qu'on a inventé, et qui d'un seul coup résoudrait l'ensemble des problèmes.

Jean-Claude BOURRET

Comment voyez-vous la cybersécurité des entreprises, en général notamment face à des évolutions technologiques comme le cloud computing.

Patrick PAILLOUX

La situation de nos entreprises, de nos administrations, de nos systèmes d'information, n'est pas bonne. Cela fait quelques années que je le dis et cela ne va pas changer du jour au lendemain. On a développé l'informatique et la société de l'information sans se préoccuper de sécurité parce que, pendant dix, quinze, vingt ans, il n'y avait pas de vraies menaces. Aujourd'hui, évidemment, on a identifié un point de faiblesse et ça va prendre du temps avant que l'on arrive à revenir à une situation plus raisonnable. Raison de plus pour commencer vite et s'en préoccuper, mais je ne crois pas qu'on arrivera à le résoudre. Donc la priorité de l'état, évidemment, c'est de commencer par les éléments les plus essentiels. L'état, ces dernières années, s'est d'abord tourné vers lui-même puis vers les infrastructures les plus critiques de la nation, les systèmes militaires etc. Si je prends l'exemple de l'ANSSI, on a commencé depuis un an maintenant à travailler vers le secteur privé. Je ne pourrais pas le chiffrer précisément, mais je dirais qu'il y a un an, un an et demi, presque 80 % de notre action était tournée vers l'intérieur de l'administration. Je pense qu'aujourd'hui 60 à 70 % au moins de l'action de l'ANSSI est tournée vers le secteur privé, donc vous voyez bien la vitesse à laquelle on évolue.

Jean-Claude BOURRET

Merci beaucoup pour votre intervention. Le dernier intervenant est monsieur Eduardo RIHAN CYPEL, député de la 8ème circonscription de Seine et Marne, membre de la commission de la défense nationale à l'Assemblée nationale et de la commission du Livre Blanc sur la défense et la sécurité nationale. Il est maître de conférence à Science Po Paris. Monsieur le député, nous vous écoutons avec plaisir.

Eduardo RIHAN CYPEL

C'est toujours un peu délicat d'intervenir en dernier quand beaucoup de choses ont été dites et ont apporté de la richesse au débat. Vous m'excuserez par avance si il y a un petit peu de répétitions. Je vais essayer de ramasser un certain nombre d'éléments dont certains ont pu être déjà exprimés ici et de vous dire ce que ces questions peuvent représenter pour un parlementaire, car je crois que c'est un point de vue qui est important compte-tenu des éléments que nous connaissons.
Alors un premier rappel, je crois que le cyber est un nouvel espace de conflictualité mais il n'est pas seulement cela, c'est un nouvel espace tout court qui envahit depuis de nombreuses années, de plus en plus, tous les segments de l'organisation sociale. Le numérique, la grande révolution du numérique qui est apparue ces dernières décennies, est une révolution sur tous les plans. C'est une révolution industrielle, une révolution du mode de production. La plupart des économistes ou des observateurs disent qu'elle est beaucoup plus importante que celle qu'a pu représenter la révolution industrielle que nous avons pu connaître au 19ème siècle et avec ses accélérations

au début du 20ème.
Dans cette grande révolution, l'impact fondamental du cyber est qu'il traverse l'ensemble des domaines de l'organisation sociale, de la vie quotidienne et de la production. C'est un enjeu majeur. Il était évident que sur le plan de la défense, de la sécurité et militairement ce soit un domaine qui bouleverse la donne sur un certain nombre de sujets. Il va de soi que si nous sommes en train d'inaugurer la 5ème édition de ce forum c'est qu'il y a une prise de conscience aujourd'hui clairement établie dans le monde de la défense et de sécurité. Il y a bien, en effet, un enjeu de défense militaire et sécurité. L'introduction du général Watin-Augouard a bien montré que dans ce continuum de défense et de sécurité il est parfois difficile, si ce n'est pour l'intérêt des besoins de l'analyse, de distinguer ce qui fait partie de la défense de ce qui fait partie de la sécurité et qu'il faut traiter tout cela d'un seul trait.

La cyberdéfense est apparue dès 2008 comme un enjeu déterminant, structurant pour notre défense, et une question stratégique. Il est évident que la question de la cyberdéfense est au cœur de ce Livre Blanc comme elle l'a été au cœur du précédent. Sans vous dévoiler les secrets, de nos travaux et de nos débats, c'est une question qui est centrale.dans le cadre des travaux du Livre Blanc auxquels j'ai participé. Dans cette version, qui devrait être finalisée début mars 2013 au plus tard, il va de soi que la question de la cyberséurité et de la cyberdéfense est d'autant plus centrale qu'elle l'est dès le départ. Si vous lisez la lettre de missions du président de la République à Jean-Marie Gehenno, qui préside la commission du Livre Blanc, la cyberdéfense et la cybersécurité sont citées comme l'un des domaines principaux sur lesquels le président souhaite que nous travaillions.
Pour ce qui nous concerne, un enjeu a été exprimé. C'est le rôle du parlementaire d'en prendre la mesure. Il y a un enjeu d'indépendance et d'autonomie pour que précisément nous puissions assurer l'ensemble des conditions qui font l'organisation de la société dans le monde cyber comme dans le monde numérique. Il y a une interdépendance de plus en plus forte à cause du numérique. On voit bien aujourd'hui que tout dépend du numérique, tout est cyber et le cyber est ce qui est un petit peu structurant dans l'ensemble des domaines. Il y a donc un enjeu d'indépendance pour que nous soyons nous même à la fois ceux qui produisent nos propres besoins en matière numérique et ceux qui nous protégent, nous sécurisent et nous défendent en la matière.
Il y a donc un enjeu pour toute la société dans son ensemble avec la numérisation. Ces enjeux sont bien entendu de défense et de sécurité mais il y a également un enjeu au niveau du simple citoyen car chacun le vit au quotidien. Le général a exprimé dans son préambule que nos sociétés, nos organisations sociales vont vers des processus de dématérialisation. Il y a donc un enjeu à pouvoir sécuriser ce qui va dans le sens de la dématérialisation, de la numérisation d'actes civils, d'administration ou légaux. Nous avons besoin de pouvoir garantir que ces actes ne sont pas piratés ou des faux. Chacun de nous reçoit des e-mails avec des tentatives pour obtenir des comptes en banque ou pour remplir tel ou tel dossier, pour donner un numéro de je ne sais trop quoi. On voit très bien, qu'avec le numérique, il y a par définition de nouveaux types d'actes criminels, de délinquance, de terrorisme aussi contre lesquels nous devons nous protéger. Il va de soi que nous ne pouvons pas protéger les renseignements les plus

vitaux pour l'État français de la même manière que les quelques données personnelles qui n'ont pas de caractère stratégique pour l'intérêt de la nation.
Il y a là pour le législateur un certain nombre d'enjeux notamment au niveau des normes, des codes et de la loi. On parle même, certains magistrats y pensent, d'un futur code cyber pour légiférer sur les questions liées au numérique. Je ne sais pas si nous arriverons à un code du numérique ou cyber mais lorsque l'on a inventé les voitures, il n'y avait pas de code de la route préalable à cette invention. Pour le numérique, c'est un peu la même chose, car s'il y a un certain nombre de domaines qui ont déjà fait d'ores et déjà l'objet de normes, je crois que nous ne sommes qu'aux balbutiements, qu'au commencement de ce nouveau monde de normes qui apparaît au fur et à mesure de l'émergence de nouvelles technologies et de nouvelles possibilités liées au numérique et au cyber. Cela sera un domaine exponentiel et mon rôle de député, qui s'intéresse à ces questions, c'est aussi de sensibiliser mes collègues parlementaires. Il y a déjà eu, on le sait, le rapport du sénateur Jean-Marie Bockel, qui interviendra au cours de ce forum, qui apporte un certain nombre de propositions très intéressantes. Mais je crois que nous avons ensemble besoin de sensibiliser l'ensemble de nos collègues parlementaires, députés, sénateurs à l'intérêt de défricher ce terrain et à poser avec l'ensemble des professionnels les questions liées à la normalisation, si j'ose dire, à la légifération de certains nombres de domaines en distinguant ce qui est essentiel, vital et décisif pour la sécurité de la nation de ce qui doit être tout simplement être régulé.
Le cyber est un nouveau domaine de régulation, qui doit rassembler toutes les normes possibles, nationales, européennes, internationales et tous les domaines de réglementations pour garantir la sécurité. Je crois aussi que le cyber, au-delà des menaces, est aussi une opportunité, formidable lorsque la France, comme l'Europe en général, traversent une crise économique sans précédent depuis les années 30. Une crise, sans doute, mais qui est aussi une mutation économique liée déjà à la réorganisation du système de production, à la révolution industrielle liée au numérique. Je crois justement qu'il y a une opportunité, pour la France en particulier, de créer de nouvelles filières économiques et industrielles à même d'apporter un nouveau cycle de richesse, de croissance, un nouveau cycle de développement avec de la valeur ajoutée et pour lequel justement nous pouvons être des précurseurs. Je crois que la France doit être à l'avant garde de la nouvelle bataille économique qui se joue dans le domaine du cyber et, de ce point de vue, le parlementaire que je suis doit pouvoir aider à la sensibilisation dans l'ensemble des domaines. Nous avons des fleurons en France, des leaders, de la technologie et des grands groupes qui sont capables d'être à l'avant-garde mais je crois que nous avons besoin de renforcer l'ensemble de cette filière qui doit être aujourd'hui construite. Il y a un risque fondamental dans ce pays. On parlait tout à l'heure de ces attaques et de ce qu'elles peuvent représenter. Patrick Pailloux a raison : les menaces, les risques ne conduisent pas uniquement à des risques virtuels. Moi, comme parlementaire, je me pose tous les jours la question de la préparation de la France contre un « *cyber 11 septembre* ».
La question, aujourd'hui, est là. Les attaques ne sont pas simplement des attaques virtuelles avec des effets virtuels. Les attaques qui peuvent être introduites aujourd'hui par un virus ou

par n'importe quelle attaque de type cybernétique peuvent avoir des dégâts et des effets matériels gigantesques. On peut s'attaquer à une centrale nucléaire, à un barrage, à notre réseau de transport, faire dérailler des trains. On peut causer des dégâts immatériels importants : imaginons une attaque contre la Banque centrale européenne, notre système bancaire ou tout simplement une attaque qui paralyserait la possibilité de faire des retraits d'argent dans la ville de Paris uniquement. On peut tout simplement paralyser du simple fait de l'interconnexion, de l'interdépendance des systèmes numériques, toute l'organisation sociale. Le général Bonnemaison l'a dit tout à l'heure, l'appareil de défense et de sécurité militaire doit prévoir un certain nombre de déstabilisations de cette nature, le risque étant naturellement asymétrique. Chacun sait ce qui a pu se passer en Iran il y a quelque temps. Le fameux virus stuxtnet a pu détruire des centrifugeuses iraniennes et retarder le programme nucléaire iranien. Cette opération n'a pas pu se faire sans une préparation en amont, et du renseignement traditionnel. Les américains ont beaucoup souffert avant et après le 11 septembre parce que beaucoup avait été investi dans le domaine du renseignement informatique, numérique en délaissant parfois le terrain. Je crois que c'est précisément l'erreur à ne pas faire. Si le numérique et le cyber montent en puissance et vont prendre de plus en plus de place dans le domaine de la sécurité, on ne peut pas, en particulier dans le domaine du renseignement, abandonner la partie traditionnelle. Nous devons réfléchir et penser l'articulation des deux composantes. Le retex de ce qui s'est passée en Libye, et bientôt, je l'espère le retex de ce qui se passe aujourd'hui au Mali, nous donnerons des informations supplémentaires pour nous améliorer dans ce domaine.

Pour conclure, je crois que toute la nation doit faire un effort et se mobiliser. L'information aujourd'hui et la préparation sont fortes. L'ANSSI se développe de plus en plus, gagne en force, y compris en ressources humaines, pour pouvoir faire face à l'ensemble des risques et des menaces. L'appareil d'état dans son ensemble commence à se mobiliser et nous avons tous conscience que cette information, cette sensibilité n'est pas toujours partagée. Les grands groupes qui sont les plus concernés par les questions de cyberguerre, cybersécurité, cyberterrorisme sont sans doute en pointe mais nous avons à sensibiliser tous les chefs d'entreprises et mobiliser tous les efforts de la Nation à la fois pour nous préparer, nous sécuriser, sécuriser en particuliers nos infrastructures vitales, mais également pour nous défendre contre toutes les formes d'intelligence économique. Il y a du travail pour être, tant en France qu'au sein de l'Union européenne, le plus indépendant possible en matière de cybersécurité et de cyberdéfense. Je crois aussi que nous devons renforcer la formation dans l'enseignement supérieur pour justement recruter suffisamment d'ingénieurs et sensibiliser l'ensemble de la société française. C'est un enjeu majeur et je crois qu'il est essentiel que la Nation se mobilise et s'approprie cette nouvelle filière industrielle et économique à laquelle je crois fermement.

Jean-Claude BOURRET

Monsieur le député, merci infiniment pour votre intervention. En guise de conclusion, mesdames et messieurs, je vous remercie de votre attention ainsi que les intervenants qui ont bien posé ces problèmes auxquels nous allons être confrontés pendant tout ce 21ème siècle.

P2 – Cyberespace, identité numérique, éthique et vie privée

Nous allons continuer ce périple à travers le cyberespace. Je suis vraiment très contente de pouvoir animer cette séance plénière où nous allons aborder le thème « *cyberespace, identité numérique, éthique et vie privée* ».
A l'ère du numérique, l'identité est une notion qui est devenue extrêmement extensible qui est même devenue floue. Évidemment, l'identité est jusqu'à présent définie et contrôlée par l'état, je pense à l'état civil. Maintenant, au vu du développement numérique, les choses ont vraiment changé et l'identité numérique n'a pas vraiment de définition, ce qui perturbe d'ailleurs en particulier le juriste que je suis. L'identité peut être le pseudo. Il y a eu un débat aussi sur l'identité et données personnelles: l'adresse IP est-elle une donnée personnelle ? L'identité numérique est au cœur d'enjeux à la fois économiques, stratégiques et au cœur d'enjeux liés aux libertés individuelles. A quoi correspond aujourd'hui l'identité numérique ? C'est ce que nous allons examiner. Cette question est évidemment fondamentale. Il faut s'adapter à une société de plus en plus numérisée mais qui doit être sécurisée. Il y a donc des équilibres à trouver et le sujet me plaît beaucoup en tant que magistrat. Il faut trouver un équilibre entre la protection vis à vis des atteintes aux libertés individuelles et le développement de cet univers numérique. Pour aborder le sujet, nous avons rassemblé les meilleurs experts que je vous présente très rapidement. Solange Ghernaouti qui est professeur, directrice du groupe de recherche cybersécurité à l'université de Lausanne, HEC Lausanne. Didier Trutt qui est président directeur général de l'Imprimerie nationale, Gwendal Le Grand chef du service de l'Expertise informatique à la CNIL. Anthony House directeur du développement stratégique des affaires publiques (Europe) chez Google et madame Marielle Gallo député au Parlement européen, membre de la Commission Juri membre de la Commission IMCO qui justement élargira le débat avec les problématiques européennes et internationales.
Je vais sans plus attendre, donner la parole à Solange Ghernaouti qui est docteur en informatique je le rappelle à l'université Paris VI, qui est l'auteur d'un nombre considérable d'ouvrages dont un « *Que-sais-je ?* », un livre de cours en sécurité informatique chez DUNOD. Elle est lieutenant-colonel dans la réserve ci-

toyenne de la gendarmerie française. Donc tout d'abord, Solange Ghernaouti, pouvez-vous nous présenter les enjeux, comment aujourd'hui, sécuriser les identités dans le cyberespace ?

Solange GHERNAOUTI

Je vous remercie pour cette question qui est une question fondamentale pour laquelle une réponse simple n'est pas possible. Pour cela, j'aimerais rebondir sur les propos tenus ce matin en guise d'ouverture de ce forum par le général Watin-Augouard. Il nous a parlé de « *partage de conscience, de prise de conscience pour une meilleure connaissance, pour agir ensemble, pour ne pas subir seul* ». Je les interprète comme la nécessité de devenir acteur de cette société d'information que nous sommes en train de construire et, pour paraphraser Saint-Exupéry, je dirai que nous n'héritons pas du cyberespace de nos ancêtres, mais que nous le construisons pour nos enfants. Nous devrions bâtir cet écosystème numérique en toute connaissance des risques, sans omettre bien sûr les opportunités possibles. Toutefois, c'est sur le côté négatif des risques liés aux infosphères que nous développons autour de notre identité numérique et de nos projections identitaires dans le cyberespace, qu'il est judicieux de s'attarder aujourd'hui. Alors que le cyberespace constitue une fenêtre d'opportunités pour le développement économique et personnel, il ne faut pas oublier qu'il est également au service du développement de la criminalité et de la profitabilité des criminels. Pour reprendre les propos du général, qui m'ont beaucoup interpellé notamment, le fait « *de ne pas perdre notre âme* », pour moi cela veut dire donner du sens au changement, ne pas le subir, mais en être un acteur à part entière. C'est pour cela qu'il faut accompagner les mutations induites par les technologies du numérique, par une appréhension holistique du phénomène, qui intègre une approche spirituelle, philosophique et culturelle. Ce qui se reflète assez bien dans le titre de cette session « Cyberespace, identité numérique, éthique et vie privée », car on ne peut restreindre cette problématique à sa seule dimension technologique, et c'est peut-être ce que nous sommes en train de découvrir. Les besoins liés à la maîtrise de l'identité numérique, à l'existence et au partage de valeurs éthiques et à la protection de la vie privée, ne peuvent être satisfaits uniquement par des réponses d'ordre théologique.

Pour comprendre l'importance des enjeux de la maîtrise de l'identité numérique et l'ampleur des défis de sa sécurité à relever, j'aimerais rappeler, brièvement, quelques aspects de l'évolution technologique en cours. Comment cela nous concerne-t-il et comment nous la favorisons ? Nos habitudes de connectivité permanente, à laquelle nous sommes de plus en plus exposés via la téléphonie mobile, les tablettes et les portables autorisent une communication interpersonnelle et interinstitutionnelle, mais il s'avère désormais que les objets sont aussi connectables à l'internet. Ils deviennent communicants. C'est l'internet des objets qui envahit progressivement notre espace domestique mais aussi notre espace public, comme par exemple avec des feux de signalisation ou encore les voitures communicantes. L'augmentation de l'ouverture des systèmes à l'internet et du nombre d'entités connectées augmente considérablement le nombre de cibles de la malveillance et globalement la fragilité de l'écosystème numérique. Ainsi la cybercriminalité croit avec le nombre d'internautes et d'entités raccordées à internet.

Force est de constater que la miniaturisation des composants électroniques, les puces RFID (Radio Frequency Identification), les nanotechnologies, les poussières intelligentes (smart dust), la prolifération de capteurs que l'on peut intégrer dans toutes sortes d'environnements, y compris dans le corps humain (notion de prothèse numérique, de fusion des mondes biologique et électronique), les communications sans fils, favorisent l'interconnexion d'équipements électroniques à grande échelle par des technologies de l'internet. On voit ainsi apparaître une potentialité de piratage importante avec des impacts sur la sécurité économique mais aussi sur la sécurité et la sûreté publique, la sécurité physique et la sécurité des individus. C'est sans évoquer l'apparition d'interfaces neuronales qui permettent de téléguider les ordinateurs par la pensée, mais aussi à l'inverse permettraient de « *pirater* » le cerveau. Ce sont des applications utiles en médecine pour augmenter les capacités de personnes souffrant de certains déficits, ce qui est bien sûr un avantage. Il en est de même de certaines approches biomédicales où la robotique mobile contribue à aider les personnes notamment âgées, comme c'est déjà le cas au Japon. Ce seraient donc des entités électroniques et informatiques, téléguidées, qui pourraient piloter notre environnement, nos comportements et nos activités humaines et ainsi les maîtriser. Sans faire de la science-fiction, ni être excessivement pessimiste, il n'est pas exclu que ces « *robots d'assistance* », ces « *poussières intelligentes* » puissent devenir la cible de malveillances et de cyber attaques et puissent avoir des comportements indésirables et devenir nuisibles. Dans une certaine mesure ce sont d'ores et déjà des applications et services informatiques qui conditionnement nos comportements, nos interactions avec autrui, qui créent des habitudes, voire des addictions.

De façon concomitante on a vu apparaître une « *massification* » des données, y compris des données personnelles, notamment par l'approche des réseaux sociaux, des blogs, etc., par cette communication extensive, par cette mise en scène de soi et de toutes les données dispersées dans des services d'informatique en nuage (cloud computing). L'ingénierie sociale, l'exploitation des données personnelles à des fins malveillantes, comme l'usurpation d'identité, se sont intensifiées ces dernières années. Rappelons que la plupart des cyber attaques réussies, y compris dans des secteurs sensibles, ont su en tirer parti. De manière quasi naturelle, le « marché » des données personnelles s'est développé, qu'il soit licite à des fins marketing, ou illicite à des fins criminelles, les données personnelles font l'objet de toutes les convoitises et de tous les trafics. Un marché noir des données personnelles existe ; l'usurpation d'identité est une réalité dont les victimes sont légion.

De manière anecdotique, je dirai que c'est probablement l'éclatement de l'affaire « *WikiLeaks* », en 2010, qui a contribué à faire prendre conscience de l'importance des données numériques et de la non maîtrise de leur protection. Mais c'est par la massification des données associée à l'usage de plates-formes de socialisation ou de certains fournisseurs de services de l'internet, considérés comme des géants dans leur domaine, que se sont révélés les enjeux économiques liés aux modèles d'affaires et aux marchés des données, basés sur leur exploitation. Pour preuve, par exemple, l'importance accordée à la publicité et au marketing, notamment basés de plus en plus sur les données de géolocalisation (données

à caractère personnel).

Au-delà de ces enjeux économiques évoquons très rapidement ceux d'ordre politique soulevés par ce nouveau territoire qu'est le cyberespace. Pour résumer, le cyberespace est désormais un lieu privilégié d'expression des conflits économiques, politiques et aussi d'ordre personnel (harcèlement, insultes, …) et des conquêtes. Le cyberespace peut être vu comme un champ de bataille pour les individus, les organisations et les États, lieu permettant entre autres, l'enrichissement, la prise de pouvoir et de contrôle, cela de manière licite ou non.

Cette parenthèse sur le panorama des principales évolutions des technologies du numérique, me permet d'insister sur l'importance de la maîtrise des données liées à l'identité numérique. Celle-ci est une notion complexe qui peut avoir plusieurs dimensions et interprétations possibles en fonction de son contexte d'utilisation. Pour certains, par exemple, elle permet l'identification nécessaire au contrôle d'accès (approche technologique), à la facturation de services consommés (approche comptable et économique) ; pour d'autres, elle permet d'être tenu responsable et redevable d'actions effectuées (approche légale) ou encore, par exemple, d'avoir une existence (approches sociale, philosophique, administrative ou commerciale).

Il très difficile de définir ce qu'est une identité numérique parce qu'au départ l'identité des utilisateurs appréhendées via des adresses (adresses IP, email, …) avait une fonction « réseau », pour acheminer les données. Puis cette identité a dû répondre à des besoins d'identification et d'authentification. En fait pour moi, en tant que personne, ce qui m'intéresse dans la notion d'identité c'est de pouvoir apporter des éléments de réponse à la question existentielle fondamentale : « qui suis-je ? ». Lorsque j'aborde la question de l'identité sur l'angle du « *qui suis-je ?* », la réponse ne peut se trouver dans un identifiant (dans une adresse) elle n'est pas d'ordre technologique car c'est vraiment une question philosophique à part entière. Les réponses pourraient être par exemple d'ordre culturel ou éventuellement religieux.

Il y a cinquante ans, j'étais déjà Solange Ghernaouti et pourtant je n'étais pas tout à fait la même et pas tout à fait une autre que celle que je suis aujourd'hui. En fait, la notion d'identité est le plus souvent restreinte à l'identité nominative attribuée à la naissance, reflétant une certaine identité familiale mais aussi administrative et légale en fonction de l'état civil et des lois du pays dont l'individu est le ressortissant.

Tout cela pour vous dire que cette notion d'identité est floue, qu'elle n'est pas stable dans le temps, que l'identité n'est pas héritée, donnée et gérée de façon universelle et unique de par le monde. Le cyberespace pose la problématique de l'identité numérique de manière globale et universelle. Une réponse unique, d'ordre technologique dont la mise en œuvre dépendrait d'entités commerciales éventuellement étrangères, irait à l'encontre de la prise en compte des besoins humains et du respect des cultures en vigueur dans les différents pays. Ainsi, par exemple, cela serait une erreur de penser qu'une adresse IPv6 puisse être une réponse optimale. Ce n'est pas une technologie particulière qui va répondre à un problème humain et sociétal. Ce n'est pas une personne morale qui doit se substituer à l'État

dans la gestion des identités de ses citoyens.

La dématérialisation de l'identité soulève de nouveaux défis relatifs à sa maîtrise (par qui, comment, qui crée des identités numériques, qui les distribue et les contrôle, doit-il exister un état civil numérique, peut-on globaliser l'identité numérique, alors que la notion d'identité est avant tout culturelle? et à sa sécurité (comment empêcher l'usurpation d'identité, l'usage criminel ou abusif et détourné des identités numériques et des données personnelles associées?).

Cela pose de nombreuses questions d'ordre politique, économique et technologique, qui ne peuvent être résolues uniquement par une seule approche technologique ou sécuritaire.

L'humain, qui devrait être au cœur du développement du cyberespace, est en fait actuellement perdu dans le cyberespace, perdu du fait qu'il ne maîtrise pas suffisamment ni les technologies, ni son identité numérique, ni les services qu'il utilise ; qu'il ne comprend pas les enjeux, globaux et à long terme, de la perte de maîtrise de ses données ; qu'il ne sait comment ses données et ses projections identitaires sont utilisées par les acteurs licites et illicites de l'Internet.

Pour ne pas trop s'attarder, ni entrer dans des détails technologiques de la protection de l'identité numérique, je considère qu'il est nécessaire qu'elle représente d'une part l'invariabilité et la variabilité de l'identité dans le temps évoquée précédemment, et qu'elle soit maîtrisée, d'autre part, par le duo constitué du propriétaire de l'identité et du fournisseur de service utilisé.

L'identité numérique devrait être « *élastique* » et varier dans le temps. Elle ne sera pas toujours la même en fonction du contexte d'utilisation et des entités impliquées. C'est en utilisant de multiples identités numériques en fonction de l'usage, en les distribuant et en maîtrisant les diverses caractéristiques réparties d'une identité numérique, qu'il faut apporter des solutions technologiques.

Il faut que la technologie offre une réponse cohérente et fiable aux acteurs concernés par la maîtrise d'une certaine identité numérique, notamment pour des applications commerciales ou de cyberadministration. Lorsque j'utilise ma carte bancaire pour faire une transaction commerciale sur le net, ce n'est pas « *qui suis-je ?* » qui est important, c'est de savoir si je suis en mesure de payer la transaction financière. L''usage de l'identité sur internet dépend vraiment du contexte dans lequel elle est mise en œuvre. Les solutions doivent s'adapter à ce besoin et, bien sûr, il faut qu'elles puissent permettre, si nécessaire, de faire un travail de police et de justice. Cela soulève des questions de responsabilités associées à cette notion d'identité.

Pour conclure, en rebondissant sur le titre de cette table ronde relatif à la vie privée et à l'éthique dans le cyberespace, j'aurais envie de rappeler que « *la vie privée doit rester privée* » et de remarquer que ce qui me choque à l'heure actuelle, c'est l'éducation que nous sommes en train de donner à nos enfants car pour les protéger sur le Net, nous leur recommandons de mentir … les seules recommandations que nous sommes en mesure de leur proposer se résument à : ne donne jamais ton nom, ton âge, ton adresse, fais de faux profils sur les réseaux sociaux, ne fais confiance à

personne, on ne sait pas qui se cache derrière un nom, une photo… Nous sommes en train de bâtir des valeurs de société basées sur la défiance et le mensonge : quel renversement de valeurs !

Cet environnement immatériel, ce cyberespace omniprésent dans lequel nos prolongeons nos activités quotidiennes, induit de facto une culture de la défiance ou la loi du plus fort prévaut le plus souvent. Je pense qu'il faudrait ré-envisager la Déclaration universelle des droits de l'Homme, qui sont des fondements de notre éthique et qui permettent d'avoir une référence entre ce qui est bien et pas bien (car même s'ils sont souvent bafoués, cela permet au moins de le dénoncer), en tenant compte du cyberespace. Un traité international du cyberespace me semble important pour notamment, mais pas uniquement, aborder les problèmes de conflits entre Etats, traiter des principes généraux relatifs aux pratiques loyales concernant les données personnelles et des aspects fondamentaux de gouvernance de l'Internet et ainsi contribuer à définir les bases d'une cyber éthique dont les principes généraux dépasseraient les barrières géographiques et culturelles des pays.

Myriam QUEMENER

Merci beaucoup pour cette introduction qui pose bien les problématiques, le point de vue du chercheur. Je vais maintenant vous donner la parole monsieur Trutt. Vous êtes président directeur général de l'Imprimerie nationale depuis 2009. Vous avez l'expérience d'une carrière industrielle et internationale notamment en Asie du Sud-Est. Vous avez été administrateur du groupe NEXTER et conseiller du commerce extérieur de la France depuis 1992. Vous êtes diplômé de l'École nationale d'ingénieur de Saint-Étienne. On voit bien que la problématique est tout à fait pluridisciplinaire, nous sommes tous concernés par cette définition, cette sécurisation de l'identité numérique. Vous allez nous parler justement de différentes identités numériques à la fois professionnelles, régaliennes. L'imprimerie nationale a mis en œuvre des initiatives tout à fait intéressantes que vous allez mettre en perspective, par rapport à des expériences qui ont lieu en Europe. Vous allez jeter votre regard également sur des domaines tout à fait essentiels de la vie sociale notamment au niveau du transport, de la santé, de l'administration, des grandes entreprises privées.

Didier TRUTT

Bonjour à toutes et à tous. Je vous remercie Madame Quemener de me permettre de partager l'expérience de l'Imprimerie Nationale, expérience acquise au quotidien aux côtés des administrations françaises et européennes, mais également en lien étroit avec les entreprises privées de grands secteurs économiques tels que la santé et le transport. Je voudrais également saluer la collaboration étroite qui s'est créée avec l'Agence Nationale des Titres Sécurisés et l'Agence Nationale de la Sécurité des Systèmes d'Information dans la sécurisation et la délivrance de titres régaliens, notamment le passeport biométrique et le permis de conduire.

Je partage le constat de Madame Ghernaouti relatif au flou qui recouvre aujourd'hui la terminologie d'identité numérique. Dans une période où se multiplient les interactions des citoyens et des entreprises dans le monde numérique, dans un environnement où les traces

et données dispersées sur la toile s'effacent difficilement et où les moyens de croisement de données numériques sont de plus en plus puissants, ce flou constitue une véritable porte ouverte à des fraudes favorisant le détournement des biens et l'usurpation d'identité.

Avant de développer les enseignements et les perspectives que nous pouvons tirer aujourd'hui des projets mis en œuvre, qui concernent aujourd'hui plusieurs centaines milliers de personnes, je rejoins les propos d'ouverture du général Watin-Augouard, et la nécessité d'une prise de conscience collective pour agir ensemble, pour ne pas subir et pour devenir acteurs de cette société que nous sommes en train de construire.

Les identités numériques sont un peu comme l'arbre qui cache la forêt ; elles ne peuvent être réellement appréhendées que si nous analysons l'ensemble de la chaîne de confiance qui est associée à chacun de ses usages, des ouvertures, des impacts juridiques sous-jacents et des conditions d'appropriation par les internautes.

Aujourd'hui, nous utilisons quotidiennement une multitude de mots de passe, login, voire des identités numériques qui nous sont communiquées par des opérateurs privés. Face au nombre croissant de demandes d'identification, la problématique est générale. Nous finissons par utiliser bien souvent le même mot de passe et il s'agit généralement d'un mot assez simple, que l'on utilise aussi bien pour des transactions qui ont peu de valeur que pour celles qui ont des valeurs importantes et pour lesquelles le risque est encore plus grand. Tout ceci ne s'opère ni dans un pacte républicain, ni dans un cadre réglementaire.

Afin de limiter mon intervention dans le temps de parole qui m'est donné, je vais m'attacher aux chaînes de confiance dans le cyberespace et dont les objectifs de l'identité numérique visent à favoriser l'interopérabilité et l'ouverture, par exemple en permettant à un internaute de pouvoir « *s'identifier / s'authentifier* » de manière sûre vis-à-vis de différents « *systèmes ou applications* ».

Nous identifions aujourd'hui trois grands types d'identités qui peuvent interagir entre elles suivant les besoins :
- L'identité d'une personne physique, dite « régalienne ». C'est celle qui est garantie par les états. Aujourd'hui, les techniques permettent à un internaute de s'authentifier via son identité numérique.
- L'identité numérique d'une personne morale et dont les droits associés impliquent la gestion de l'identité d'une personne physique.
- Enfin, l'identité numérique d'une personne physique dans un contexte professionnel, par exemple les professionnels de santé ou encore les avocats.

L'identité professionnelle en France, précurseur en la matière, s'est développée depuis le début des années 1990 avec notamment le grand projet de Carte de Professionnel de Santé qui a accompagné la montée en puissance du projet SESAM/VITALE (dématérialisation de plus d'un milliard de feuilles de soins par an) et qui garantit dans l'ensemble du cyberespace santé la reconnaissance et l'assurance que l'internaute, qui se trouve de « *l'autre côté de la toile* », dispose des droits d'un praticien, qu'il s'agit d'un vrai praticien, et que cela pourra être démontré dans le temps si nécessaire. Dès le début des années

2000, l'identité numérique a connu également, dans le secteur du transport, une grande avancée sous l'impulsion d'un règlement européen relatif au tachygraphe numérique. Ainsi, dans l'espace européen élargi, chaque conducteur de transports de marchandises et de voyageurs, ainsi que l'ensemble des entreprises, disposent aujourd'hui d'une carte électronique professionnelle (environ 800.000 conducteurs et 55.000 entreprises en France). Je reviendrai tout à l'heure sur les questions de l'interopérabilité et sur les enseignements que nous pouvons tirer de ce projet qui est opérationnel dans plus de 33 États depuis plus de 10 ans.

Les administrations françaises sont également en train de déployer des cartes professionnelles. J'ai remarqué qu'il y avait beaucoup de gendarmes dans la salle. Je tiens à souligner que ce sont les premiers à avoir déployé cette carte professionnelle. Aujourd'hui, le déploiement s'organise, également pour la police, ou encore dans le secteur de la justice et dans un futur proche la défense, sans omettre également l'identité professionnelle dans les entreprises. Lors d'un échange récent avec un très haut responsable du Ministère de l'Intérieur, ce dernier me faisait état de sa satisfaction de la réussite du déploiement de ces cartes aux 180.000 fonctionnaires d'un grand corps. Lors de cet échange, je me suis permis de lui dire que les enjeux de l'identité professionnelle dépassaient les seules administrations et concernaient l'ensemble des secteurs économiques. A titre d'exemple je lui ai présenté le déploiement que nous avons réalisé pour un grand opérateur télécom français et là aussi, cela concerne plusieurs centaines de milliers d'employés dans le monde entier.
Ces quelques exemples concrets d'identité professionnelle intègrent un certain nombre de sécurités, notamment pour protéger nos accès physiques, nos accès informatiques indispensables pour créer la confiance dans la dématérialisation des documents et des transactions.

Pour conclure, je souhaiterais aborder les questions liées à l'identité citoyenne. Je ne sais pas si c'est la définition la plus appropriée, mais en tous cas elle est d'actualité avec les débats européens relatifs à l'identité numérique des personnes physiques. L'idée est que chaque citoyen européen puisse avoir une identité numérique reconnue par l'ensemble des Etats de l'Union et qu'elle soit directement équivalente et transposable à l'identité physique. Il s'agirait d'avoir la possibilité d'associer des informations numériques non falsifiables à une personne physique ou à son état civil. Un certain nombre de projets ont été déployés en Europe, notamment en Allemagne, en Espagne, ou encore en Belgique, ou Lettonie, pays qui ont aujourd'hui décidé de déployer une carte nationale d'identité numérique. D'autres pays comme l'Autriche ou la Suisse n'utilisent pas le support carte, mais d'autres supports tels que des clés USB qui contiennent une identité numérique. Quand on regarde de plus près ces identités numériques, dont les supports peuvent être multiformes, on se rend vite compte que les mêmes technologies cryptographiques associées à un code PIN sont utilisées. Dans les faits, les vrais problèmes qui sont posés concernent l'organisation et la répartition des missions et des responsabilités de la chaîne de confiance, en partant de l'enrôlement jusqu'aux usages, et des relations de cette identité numérique avec le monde de l'acceptation dans le cyberespace, qui relève du domaine public ou privé. Cette dimension de confiance réciproque ne

repose pas uniquement sur la technologie mais aussi sur l'écosystème. Il revient à l'ensemble des acteurs de créer les conditions de la réussite de cette ambition collective. En l'absence de cohérence et de niveau de garantie, de sécurité et d'interopérabilité au niveau national mais également plus largement au niveau européen, il n'y aura ni protection, ni développement de l'économie numérique.

Enfin, je souhaiterais rappeler quelques pré-requis que nous avons identifiés au regard de nos expériences : préserver le principe d'un usage volontaire, que le citoyen puisse l'utiliser quand il en a besoin et disposer d'une information précise sur l'usage qui est et qui sera fait de son identité numérique. Il faut que cela soit facile d'emploi, presque aussi facile que l'utilisation de votre carte bancaire ou de votre carte Vitale. J'ai déjà mentionné l'importance de l'interopérabilité, mais j'insisterai aussi sur le fait que l'interopérabilité n'a de sens que si la confiance existe. Ces exigences, et les réponses des procédures et organisations apportées, ont fortement marqué la réussite de projets comme celui du chronotachygraphe. Enfin, je terminerai sur l'importance des usages car c'est à travers ces derniers que le déploiement où l'utilisation de cette identité numérique verra vraiment le jour.

Myriam QUEMENER

Merci beaucoup. Quels sont les atouts de la France pour relever ces défis liés à l'identité numérique ? Parfois, on a tendance à dire que c'est mieux ailleurs. Je sais par exemple qu'au niveau législatif, on a un système, un arsenal qui fait même des envieux à l'étranger, on a même une nouvelle infraction réprimant des problématiques liées à l'usurpation d'identité en ligne. Quels sont nos atouts par rapport à la coopération publique/privée ? Que pouvez-vous nous dire sur ce point ?

Didier TRUTT

La France a énormément d'atouts. Il ne faut pas oublier que la France a été précurseur en matière d'identité numérique depuis plus de 30 ans, que cela soit dans le secteur bancaire ou encore dans le secteur de la santé. Ces réussites se sont appuyées sur notre tissu industriel de pointe. En effet, nous avons en France des industries leaders sur leur marché, que cela soit au niveau des « *fondeurs* » qui fabriquent les puces ou des sociétés de services développant les logiciels. Nous avons -et ceci grâce notamment à la réussite de grands projets, santé / transports -une véritable réflexion sur la mise en œuvre, les missions et les responsabilités d'Autorités de Tiers de Confiance, composante indispensable pour créer les conditions de la réussite de tel projets, instance indépendante garantissant l'identité numérique vis-à-vis des opérateurs publics ou privés offrant des services aux internautes. Ce dispositif est complété par de nombreux référentiels émis par des organismes indépendants et disposant d'une forte autorité et compétence, je pense notamment à l'ANSSI en matière de définition des exigences en matière de règles de sécurité (RGS), mais également à la CNIL avec qui nous travaillons quotidiennement afin que les systèmes mis en œuvre offrent tous les garanties en matière de protection de la vie privée. Certes, nous pouvons regretter les « balbutiements » que nous avons connus autour des débats sur la Carte nationale d'identité électronique, mais nous disposons aujourd'hui d'un véritable tissu industriel qui jouit d'une véritable visibilité, qui

est très présent dans de nombreux pays dans le monde et qui poursuit son déploiement. Nous bénéficions là, issu des réussites et échecs de ces projets, d'un véritable benchmark de ce qu'il faut faire et ne pas faire.

Mais je rappelle, qu'au-delà des technologies, l'enjeu, c'est la société que nous sommes en train de construire, et je suis persuadé, que nous avons la volonté politique de déployer en France les systèmes d'identité numériques.

Myriam QUEMENER

La transition est faite avec la CNIL, donc Gwendal LE GRAND est chef du service de l'expertise de la CNIL depuis avril 2007. A ce titre, vous participez aux activités du groupe des CNIL européennes, dans le cadre du G29. Avant de rejoindre la CNIL, vous étiez maître de conférence à l'École supérieure de télécommunication, vous avez obtenu un doctorat en informatique de l'université Pierre et Marie Curie en 2001.

Gwendal LE GRAND

Je vais vous parler essentiellement de l'évolution du paysage de la protection des données au niveau européen. La CNIL est compétente dès lors qu'il y a un traitement de données à caractère personnel. Cela touche les entreprises et le secteur public. Cela concerne aussi bien les services en ligne que les cartes d'identités qui sont mises en œuvre par l'état ou plus généralement les titres d'identité mis en œuvre par l'état, ou encore la « *carte agent* » qui était évoquée tout à l'heure. 2013 sera une année décisive pour la protection des données personnelles parce que tous les espaces géographiques sont en train de réviser les instruments que ce soit l'Union européenne (je développerai dans la suite de ma présentation), le Conseil de l'Europe avec la convention 108 qui est actuellement en train d'être également révisée ou l'OCDE qui travaille à la modernisation de ses lignes directrices adoptées au début des années 80. Pourquoi ces modifications ? Parce que le paysage technologique a évolué et qu'il est devenu nécessaire de moderniser ces instruments.
Au niveau de l'Europe, l'enjeu est très simple, l'Union européenne doit montrer qu'elle est capable de rénover ses instruments tout en gardant ce qui a fait sa spécificité. Sa spécificité c'est une approche où l'utilisateur est au centre, une approche où on a un très haut niveau de protection des données à caractère personnel et finalement une approche assez humaniste de la protection des données personnelles. Évidemment cette modernisation se fait avec les entreprises, les entreprises à qui on explique que la protection des données personnelles ce n'est pas seulement un coût mais aussi un investissement. Et c'est ça finalement qui permettra de créer une synergie entre protection des droits fondamentaux d'un côté et innovation technologique de l'autre. C'est d'ailleurs un des points d'attention du législateur européen dans le projet qui est en train d'être étudié.
Pour y parvenir, la France et l'Europe, s'appuient aujourd'hui sur un certain nombre de bases solides. Une base légale, puisqu'il y a une directive européenne sur la protection des données personnelles qui date de 1995, une directive de 2002 dite directive vie privée et communication électronique. La directive de 1995 est transposée en France par la loi informatique et libertés qui définit les règles relatives aux traitements de données à caractère personnel et l'ensemble des droits dont béné-

ficient les personnes. Il y a aussi une base institutionnelle puisque dans chaque État européen, il existe une autorité indépendante ; en France évidemment vous savez que cette autorité est la CNIL. La particularité de la CNIL, c'est la compétence qu'elle a développée depuis six ans environ sur le plan technologique. En effet la CNIL s'est dotée d'un service d'expertise technique dont les compétences sont reconnues par ses homologues au niveau européen et international. On travaille sur tous les sujets dans le monde de l'Internet comme dans beaucoup d'autres domaines. Cette compétence est la raison pour laquelle nous nous sommes vus confier au début de l'année 2012 par nos homologues, le dossier Google. En effet, début 2012 Google a annoncé une modification de sa politique de confidentialité et a fusionné les politiques de confidentialité d'une soixantaine de ses services. Le groupe de l'article 29 (qui est le groupe des CNIL européennes) a tout de suite décidé de se pencher sur cette nouvelle politique pour comprendre quelles étaient ses implications en matière de protection de données et vérifier si le droit européen était ou non respecté. Le G29 a désigné la CNIL comme autorité chef de file pour conduire cette analyse. En octobre, un courrier a été envoyé à Google ; il était signé par 27 autorités européennes. Dans ce courrier, les autorités présentaient les conclusions de leur analyse au regard droit européen. En particulier, les autorités demandaient à Google une meilleure information, un meilleur contrôle pour les utilisateurs sur la combinaison des données et la définition de durées de conservation. Ces demandes étaient accompagnées d'un certain nombre de recommandations très pratiques à Google. Il a été donné quatre mois à Google pour se mettre en conformité, c'est-à-dire qu'ils ont jusqu'au 15 février 2013. Ce dossier est extrêmement important pour nous aussi bien sur le plan opérationnel que sur le plan politique. En effet, c'est la première fois que les 27 autorités européennes sont d'accord sur un dossier opérationnel.

C'est également un dossier stratégique sur le plan politique, parce que cette coopération dans le cadre du dossier Google est un test par rapport au mécanisme pressenti de collaboration égalitaire entre autorités, pressenti dans le futur règlement européen actuellement en discussion au Parlement européen. Ce projet de règlement a été proposé par la Commission européenne début 2012 et il a vocation à venir remplacer la directive de 1995. Dans les grandes lignes, quels sont les points les plus importants de ce texte ? Tout d'abord, c'est une simplification pour les entreprises : vous savez qu'en France quand vous traitez des données personnelles, dans bien des cas, les traitements de données personnelles doivent être déclarés à la CNIL. Le projet de règlement, dans la plupart des cas, va supprimer cette formalité préalable. Ensuite, on va responsabiliser les entreprises, c'est-à-dire qu'on leur explique : « *la protection des données personnelles, ça va passer par vous* ». C'est le principe anglais d' « *accountability* ». Sur la compétence des autorités, le projet de règlement sera applicable dès lors qu'un résident en Europe sera concerné. Il s'agit d'un grand changement par rapport au projet initial de la Commission européenne qui prévoyait que la compétence revienne à l'autorité correspondant à un établissement du responsable de traitement dans un pays européen. Concrètement, si une entreprise était basée dans un Etat membre, l'autorité de ce pays là était compétente et pas les autres. Quand il y avait plusieurs établissements, on

désignait un établissement principal et seule l'autorité de cet établissement principal était responsable. C'est ce qui a été appelé « *le guichet unique pour les entreprises* ». Le problème est que l'autorité qui n'est plus compétente du fait de l'autorité de l'établissement principal se voit réduite à un rôle de boîte aux lettres. Ce système fragilise évidemment les droits des citoyens puisqu'un citoyen peut devoir faire un recours devant une juridiction étrangère. Mais, comme la protection des données est un droit fondamental, il faut aussi un guichet unique pour les personnes : le rapporteur du Parlement européen a proposé que le ciblage devienne un critère de compétence des autorités en plus du critère de l'établissement. Concrètement: une société est établie en Europe et va cibler des internautes dans plusieurs pays européens ; alors, les autorités des pays dans lesquels les citoyens sont ciblés peuvent également être compétentes. Comme il y a plus d'autorités compétentes, il faut un mécanisme de coopération. On a donc une autorité chef de file, une coopération entre pairs qui se met en place et un mécanisme de décision partagée entre ces différentes autorités.

Dernier point important du projet de règlement : il faut donner aux autorités les moyens de faire appliquer les règles. Concrètement: il s'agit de leur permettre de sanctionner si les règles ne sont pas respectées. Vous savez sans doute que les pouvoirs de sanction financière de la CNIL sont relativement limités aujourd'hui puisque l'on peut donner un maximum de 150 000 € d'amende et 300 000 € d'amende en cas de récidive. Le projet de règlement propose un changement d'échelle, parce qu'il permet des sanctions allant jusqu'à 2% du chiffre d'affaire mondial consolidé. C'est un chiffre suffisamment significatif pour sensibiliser les responsables des grandes entreprises aux questions de protection des données.

D'autres principes que je n'aurai pas le temps de présenter en détail sont également décrits dans le projet de règlement, comme le droit à l'oubli, le droit à la portabilité (le droit à la portabilité la possibilité de confier vos données à un acteur et de les récupérer à tout moment, dans un format standard, vous permettant ainsi d'être captif), les transferts internationaux et aussi la question des actes délégués d'implémentations, c'est-à-dire la possibilité pour la Commission européenne de venir préciser les principes du projet de règlement.

En conclusion, vous l'aurez compris, 2013 est une année décisive pour la protection des données personnelles. Un projet de règlement est actuellement en discussion au Parlement et un vote est prévu fin 2013, début 2014. La CNIL est particulièrement mobilisée pour préserver les acquis et garantir la préservation d'un haut niveau de protection des données. Enfin, sur un plan plus pratique , du fait que beaucoup parmi vous sont amenés à décider des conditions de mise en œuvre de traitements de données à caractère personnel, je vous invite fortement à consulter les guides sécurité publiés par la CNIL en 2010 et 2012 (partie 1, partie 2). Ces guides sont très utiles pour déterminer les bonnes mesures à prendre et à mettre en place dans vos systèmes pour garantir la protection des données à caractère personnel.

Myriam QUEMENER

Merci beaucoup pour cette intervention. 2013 sera certainement une cyber année, parce qu'il y a des évolutions de pratiques, des évolutions législatives et cette nécessité, comme je le disais en introduction, d'une coo-

pération publique/privée. On ne peut pas travailler chacun dans son coin mais ensemble. On a parlé à l'instant de Google. J'ai le plaisir de présenter maintenant Anthony House qui est directeur du développement stratégique des affaires publiques de Google en Europe, plus spécialement en charge des questions de sécurité et de vie privée. Vous avez rejoint Google en 2006 et vous avez été en charge des divers produits et thématiques comme notamment la lutte contre la fraude au clic, sujet tout à fait d'actualité, et au développement d'Android. Avant de rejoindre Google, vous avez obtenu un doctorat en histoire sur des effets du droit de la propriété britannique sur la croissance de Londres à l'époque moderne. Je vous cède la parole, merci.

Anthony HOUSE

Je commencerai par m'excuser d'être anglophone, mon doctorat en histoire moderne m'a aidé pour la compréhension du français pratiqué au Royaume Unis jusqu'à la fin du 14 eme siècle, période à laquelle le Parlement anglais cessa de rédiger les lois en français.
Je suis vraiment content d'être présent ici, heureux aussi d'être avec des gens aussi différents pour débattre de cette question. Nous avons coutume de dire chez Google « Si le seul instrument dont vous disposez est un marteau, vous traiterez tout comme un clou ». Vous cherchez des solutions pour régler les problèmes en fonction des outils dont vous disposez. C'est ici l'occasion de saluer les organisateurs de cette conférence qui aborde cette importante question sous des angles d'attaque aussi divers.
Je pense que le point de départ, pour Google, est que la capacité à innover et une utilisation responsable des données peuvent profiter à la fois aux individus et, de manière plus générale, à la société. J'aimerais mettre l'accent sur quelques exemples de choses que nous avons réalisées ces dernières années et qui mettent cela en évidence.

Il se peut que certains d'entre vous connaissent ce que l'on appelle l'indicateur de propagation du virus de la grippe (Goggle flue trend). Il s'agit de l'observation de données agrégées par Google de certaines régions, comparées avec des données épidémiologiques données par différents services de santé nationaux. En remarquant les corrélations, en fait, nous avons été amenés à émettre des hypothèses sur les déclenchements de grippes par régions et par secteurs. Dans la plupart des cas, ces prévisions, si elles sont très précises, permettent également d'obtenir la tendance avec deux semaines d'avance par rapport à une étude épidémiologique standard. Aussi, pour tenter de mettre un terme à la propagation d'e l'épidémie, l'utilisation de ce type de données agrégées ne peut être liée à un individu. En effet, cette démarche ne permet pas d'identifier une personne atteinte de la grippe, mais permet d'identifier les symptômes grippaux au sein d'une population donnée.

Nous avons pu établir que ce type de corrélation s'applique aux indicateurs économiques. Les économistes de renom appellent cela « prédire le présent ». De la même manière, en observant les données agrégées, il est tout à fait possible d'apprécier ce qui attire le consommateur à un moment donné sans avoir à attendre plusieurs semaines pour disposer des données collectées ou analysées

. En réalité, cela nécessite peu d'ajustements par la suite. Ainsi, étant capables d'apprendre plus à partir de cette observation nous pouvons mieux évaluer l'état de la situation économique ou bien encore certaines de ses composantes qui posent problème, le tout en un très rapide tour d'horizon.

Il y a également des instruments qui apportent une aide considérable aux personnes. L'un de ceux que j'utilise souvent est « Google cartographie et itinéraire » (Google map and navigation). Les gens qui utilisent Google map sur leur téléphone mobile ont la possibilité de ne pas dévoiler leur localisation avec le service que Google propose. En disposant de cette information de localisation en temps réel, nous pouvons créer des cartes routières pour un nombre beaucoup plus important de rues. Ceci signifie que nous pouvons offrir aux personnes des propositions d'itinéraire sur leur téléphone qui sont simplement un temps moyen de trajet. Ce n'est pas tant le trajet le plus court pour aller d'un point A à un point B qui importe mais l'itinéraire le plus rapide pour aller du point A vers le point B à l'instant t.

Cela peut être vraiment intéressant pour un individu mais cela peut l'être plus encore en cas d'urgence; pour, si nécessaire, reconnaitre les voies possibles d'évacuation dans les grandes villes. Ces types de technologies et d'analyses de données peuvent être utiles à la fois aux individus et plus largement à la société. Mais il y a un important préalable : nous avons besoin de nous assurer que ces données sont utilisées de manière responsable.

D'un point de vue éthique, nous pourrions appeler cela intérêt personnel bien placé. Google et les autres sociétés de technologie ont besoin de nouer une confiance avec les utilisateurs si ceux-ci veulent continuer à utiliser leurs services. Et comme Google et les autres entreprises compagnies du web sont en grande partie liées à la circulation de l'information, leurs capacités à résister est basée sur le nombre de personnes qui souhaitent leur faire confiance avec des informations. Je pense que l'apprentissage de ces nouvelles technologies est une question majeure pour la société et, comme nous nous sommes familiarisés avec les nouvelles technologies, nous décidons ce que sont les règles fondamentales d'éthique tant pour leur utilisation que pour ceux qui fournissent ces services. Il y a actuellement à Bruxelles un processus en cours lié à la régulation de la protection d'avoir des centaines de millions de des données, qui est, de manière générale, une discussion de société. Google a vraiment la chance personnes qui utilisent ses différents services. Nous avons la responsabilité de protéger cette information mais également de respecter de manière très sérieuse les règles prévues par la loi. Je veux simplement évoquer certaines choses que nous avons faites au sein de la grande communauté internet.

Nous étions le principal fournisseur d'accès au web à offrir pour tous nos services de protocole SSL par défaut. Autrement dit, personne ne peut pirater la ligne. Nous sommes l'un des premiers à avoir adopté la double authentification. Ce n'est pas simplement le mot de passe qui pourrait être le même que vous utilisez pour votre établissement bancaire ou votre service de vidéo à la demande, mais il y a autre chose dont vous disposez dans cette procédure de double authentification, c'est un

code qui vous est envoyé sur votre téléphone. Ou bien vous utilisez quelque chose qui permet de générer un code, même si votre mot de passe connu est compromis. De ce fait, il est moins évident et plus difficile de compromettre votre compte et, par conséquent, votre identité.

Nous avons mis en place une industrie leader dans le domaine protection-sécurité par le biais du navigateur appelé Google Chrome. Mais je pense que notre responsabilité dépasse l'utilisation qu'ont les gens de nos services et la confiance qu'ont les gens dans le web. Comment la technologie réussit-elle à protéger les informations personnelles?
Nous travaillons avec une équipe d'Harvard sur un projet appelé "Stop Badware " qui a pour but de prévenir et d'empêcher la prolifération de virus et autre Malware. Nous offrons un programme de navigation sécurisé appelé API permettant à n'importe quel site ou navigateur de créer les moyens de protection que l'on trouve dans Google Chrome pour avoir accès à nos services.
Je pense tout particulièrement à la question de l'identité. Nous collaborons activement avec l'organisation Open ID, qui est à but non lucratif aux Etats-Unis, et qui a développé des technologies comme "OAuth " qui permettent à un utilisateur de se servir de ses identifiants pour se connecter en toute sécurité.

La dernière chose que je voudrais dire avant de conclure est qu'il faut s'assurer que l'accès légal par des chercheurs aux données personnelles de nos services soit réalisé de manière cohérente et évidente. Ainsi nous précisons quels sont les types de données utilisateurs qui peuvent être fournies et ce, face aux différents systèmes juridiques tels que les assignations à comparaitre, les ordonnances délivrées par les juges, les mandats de perquisition signé par les juges.
Nous sommes une des seules entreprises à opérer avec clarté. Depuis une demi-douzaine environ d'autres sociétés ont commencé à publier ce type de document et des gouvernements ont manifesté leur intérêt pour la publication de leur rapport sur les demandes interprofessionnelles de données–utilisateurs. Simultanément, nous sommes engagés tant avec le privé qu'avec les différents gouvernements à travers le monde pour garantir les règles d'accès légales, c'est-à-dire le respect de la loi, le respect des principes de proportionnalité et de justice pour s'assurer que les gens sont correctement protégés par les mêmes droits que ceux donnés au cours des siècles.

Myriam QUEMENER

Merci beaucoup pour cette présentation et nous allons passer maintenant à la dimension européenne. Marielle GALLO, vous êtes député au Parlement européen. Vous avez été présidente du groupe de travail « *copyright* » du Parlement européen qui a terminé ses travaux en juin 2011. Je pourrais citer un certain nombre de vos activités, vous êtes même écrivain et vous avez à la suite du succès de ce groupe de travail, lancé IP Forum en novembre 2011 qui a pour objectif de susciter le débat entre les parties prenantes, les experts, les responsables politiques. C'est très intéressant d'avoir votre éclairage en tant que député européen et, ce qui est aussi essentiel, c'est que vous nous présentiez ces travaux au niveau européen. Vous allez probablement nous parler du règlement sur la protection des données personnelles et également de ce centre euro-

péen qui vient de s'ouvrir et qui est basé à La Haye.

Marielle GALLO

Merci, je suis toujours très heureuse en tant que député européen de rendre compte aux citoyens français de ce qui se passe à Bruxelles et de l'état de nos travaux parce que cela me donne l'occasion de leur rappeler que 75% de nos lois nationales sont conçues à Bruxelles et finalement dans l'ignorance et l'indifférence la plus totale puisque même les citoyens français oublient pendant cinq ans au moins, qu'ils ont élu des députés européens qui sont là-bas pour défendre leurs intérêts.

Je me situe effectivement dans une perspective européenne et j'aime bien les chiffres. Quelques chiffres en ce qui concerne l'Europe: 89% des utilisateurs en Europe ne souhaitent pas divulguer leurs données personnelles, 74% d'entre eux estiment que le risque d'être victime de cybercrime a augmenté en un an, c'est l'euro-baromètre de juillet 2012. Au premier trimestre 2012, des fraudeurs ont vendu en ligne 12 millions de données personnelles, donc on est vraiment pas dans le fantasme. En juillet 2012, comme tout le monde le sait, Yahoo a dévoilé le vol de 450 000 mots de passe de ses utilisateurs. Voilà un constat chiffré en Europe. Je pourrais rallonger la liste mais cela n'est pas nécessaire. S'agissant de la prise de conscience de certains États membres, je vais citer le Royaume-Unis qui a vraiment mis au point une stratégie pour lutter contre la cybercriminalité en novembre 2011 et qui a affecté 800 agents à ce travail. En Allemagne, 80 millions € de crédits et 500 agents sont consacrés à une stratégie lancée en février 2011. Je sais que la France n'est pas à ce niveau, elle n'est pas en retard non plus avec la création de l'ANSSI en 2009 mais par exemple en France, nous n'avons que 230 agents qui s'occupent de la lutte contre la cybercriminalité. Je ne m'occupe pas des problèmes français mais je tiens quand même à le signaler. En Europe, on a pris conscience du fléau de la cybercriminalité, on a constitué une Commission spéciale qui m'a donné l'occasion d'inviter madame Myriam Quemener. Cette Commission n'est pas seulement axée sur la cybercriminalité puisque qu'elle traite des crimes organisés, de la corruption et du blanchiment de fonds. Mais au sein de cette Commission spéciale, nous avons étudié les questions de cybercriminalité. Je me réfère également à la déclaration de notre vice-président de la Commission et commissaire à l'agenda numérique, Neelie Kroes, qui a fait une déclaration au Financial Times, le 22 janvier dernier, pour dire qu'il fallait obliger justement les réseaux sociaux, les entreprises d'e-commerce et les plateformes à déclarer les fuites et les attaques. C'est une prise de position très claire.
Mais nous observons en Europe comme ailleurs c'est le titre d'ailleurs de cette table ronde un grand dilemme entre respect des droits fondamentaux et les nécessaires régulations. Avant d'en venir aux textes actuels sur lesquels nous travaillons, je voudrais mentionner parce que ça m'a quand même beaucoup frappée, je voudrais mentionner la directive de 2010 qui était consacrée à l'exploitation et aux abus sexuels concernant les enfants et la pédopornographie. La question portait sur la suppression de pages sur internet et le blocage d'accès. Chacun aurait pu penser que tout le monde était d'accord pour procéder de cette manière. Il a fallu des mois et des mois pour arriver à ce résultat. Ce qui veut dire qu'il y a

eu une résistance au-delà d'une résistance idéologique d'une certaine communauté internet que je connais. Il y a eu une résistance terrible de la part des citoyens qui ne veulent pas qu'on attente à leur vie privée. Ils se disent que si l'on peut supprimer des pages ou bloquer un accès pédopornographique, on peut le faire pour eux également. On le constate par exemple en Pologne ou dans les anciens États soviétiques, les États Baltes, etc. Parce qu'ils ont connu le joug, la dictature, ils ont une peur bleue d'un internet sécurisé. Donc, tous les textes que nous arriverons à voter seront des textes fondés, comme d'habitude, sur un consensus. Il faut tenir compte de cet état d'esprit de ces pays où, tous groupes politiques confondus, de l'extrême droite à l'extrême gauche, c'est la même position de méfiance envers l'état dont je viens de vous parler.

Je parlais de cette directive mais puisqu'elle est de mars 2010, elle est ancienne. Je veux parler des initiatives récentes en ce qui concerne l'Europe, car je crois que l'espace européen est le seul pertinent, vraiment pertinent pour la lutte contre la cybercriminalité. Aujourd'hui, franchement ça n'est plus à la portée d'un état de lutter seul contre des cybercrimes qui sont évidemment sans frontière.

Donc un mot d'abord de la création de ce centre européen de lutte contre la cybercriminalité. C'est extrêmement récent puisque est né d'une communication de la Commission en date du 28 mars 2012. Il va commencer à être opérationnel. C'est un office qui dépend de Europol et qui va constituer le point focal européen dans la lutte contre la cybercriminalité. Évidemment il va se concentrer sur les activités illicites en ligne menées par des groupes organisés et, plus particulièrement, sur celles qui génèrent des profits considérables comme la fraude en ligne impliquant le vol des détails de comptes bancaires et des cartes de crédit. Ce centre européen sera aussi une plate-forme pour les enquêteurs européens, les entreprises privées, les chercheurs et les associations d'utilisateurs. Et puis ce sera un partenaire dans les interactions avec les autres acteurs internationaux extérieurs à l'Union européenne. C'est donc une initiative extrêmement importante et on en attend beaucoup.

S'agissant du règlement pour la protection des données à caractère personnel. Le représentant de la CNIL vous a dit beaucoup de choses que je ne vais évidemment pas répéter, sauf à préciser que je suis rapporteur à la Commission des affaires juridiques sur ce texte. Ce qui est très important et vous l'aurez bien compris, c'est qu'il s'agit d'un règlement et non pas d'une directive. Il n'y aura pas les aléas de la transposition. Le texte sera d'application immédiate dans les 27 États membres et ça c'est extrêmement important.

Ce texte renforce les droits du citoyen. Je ne suis pas de ceux qui ont la tête dans les étoiles et qui croient que nous allons être complètement protégés et que le risque zéro sera atteint. Par exemple, en ce qui concerne la disposition importante sur le droit à l'oubli numérique, nous savons très bien que, sur un plan technologique, c'est impossible. Donc, je crois qu'il est malsain de raconter des histoires aux citoyens et de les induire en erreur sur ces dispositions. Elles sont destinées à les protéger, oui, mais de la même façon qu'il y a toujours des gens qui font des « *fric-frac* » dans les maisons, il y aura toujours des attaques et des fuites concernant les données personnelles. On n'atteindra pas la perfection mais on essaie d'y arriver. Ce texte on vous l'a dit aussi, renforce les obligations des responsables des

traitements et des sous-traitants, question très difficile d'ailleurs, je ne vais pas entrer dans le détail. C'est une question d'ailleurs très juridique, celle des relations entre les responsables du traitement et les sous-traitants. Parfois il y a tellement de sous-traitants qu'on ne sait plus qui était le responsable du traitement.
Sur les sanctions, comme on vous l'a dit, elles ont été considérablement augmentées. Mais personnellement, j'ai quand même souhaité que ce soient des plafonds parce que un million d'euros et 2% du chiffre d'affaires c'est quand même considérable. Là aussi il faut trouver un juste équilibre entre la protection des données des citoyens et le fonctionnement de nos sociétés commerciales qui utilisent internet. On ne peut accepter qu'une législation tellement lourde et tellement coûteuse, le marché intérieur européen ne soit plus compétitif et se fasse attaquer une fois de plus par les américains et les chinois. Là aussi, il faut trouver une juste mesure et ce n'est pas si facile que ça.
Sur ce règlement, il y a un grand progrès en ce sens que l'on va pratiquer pour les autorités de contrôle ce que l'on appelle le « *one stock shop* », c'est-à-dire une autorité chef de file,. Personnellement et là je pense que je serai suivie, j'ai déposé des amendements pour que les autres autorités des autres États membres ne soient pas que des « boites aux lettres », dans la mesure où le citoyen recourt à l'autorité de son pays. Donc, il faut qu'il y ait une obligation de coopération. Oui pour le chef de file, mais obligation de coopération pour les autres autorités!
Sur le règlement « *identification électronique et service de confiance* » pour nos transactions électroniques, c'est un règlement donc un texte d'application immédiate également. Là aussi, il faut que le marché intérieur arrive à exporter le potentiel que l'on a en économie numérique sinon une fois de plus, nous serons affaiblis par la concurrence.
Ça n'est pas le principe d'harmonisation qui a été choisi et Dieu merci! C'est le principe de reconnaissance mutuelle: reconnaissance mutuelle des systèmes d'identification ou d'authentification des moyens. La question reste posée et elle va être débattue. Je suis rapporteur sur ce texte mais à la Commission du marché intérieur. Nous nous sommes beaucoup battus avec l'autre Commission du marché international pour avoir la compétence au fonds. Nous n'avons pas réussi, mais nous restons quand même saisis pour avis.

Ce règlement créé donc un marché intérieur des signatures électroniques et des services de confiance en ligne qui leur sont associés en garantissant un fonctionnement transnational de ces services et c'est très important en leur conférant le même statut juridique que les formalités effectuées sur les documents physiques et classiques. C'est vraiment un grand pas en avant et ce règlement va permettre aussi d'exploiter pleinement non seulement le potentiel en matière numérique mais le potentiel lié aux dispositions relatives au marché public et cela va ouvrir de grands horizons et c'est donc extrêmement important. Comme dans la proposition précédente de règlement, il y a à mon sens trop d'actes délégués, puisque, dès qu'il s'agit de passer à la disposition concrète et la mise en œuvre, la Commission se réserve un acte délégué ou un acte d'exécution. Cela prive le Parlement de la possibilité de réfléchir d'une manière démocratique sur la question et je ne vois pas pourquoi ? Nous considérons au Parlement qu'il y a trop d'actes délégués relatifs à cette question. Dans ce règlement il y a aussi un problème qui va se poser puisque la proposition de règlement prévoit la gratuité

pour tous ces services. Bien entendu, en ce qui concerne le secteur privé, il y a des résistances. En conclusion, je constate -mais je le savais depuis longtemps, parce que je suis avocate depuis 35 ans- que le droit est toujours terriblement en retard sur la technologie et ça c'est vraiment un désastre, que ce soit au niveau Français et même au niveau européen. Je pense qu'il faut lutter contre cette idéologie quand il s'agit d'une idéologie qui s'oppose à toute régulation sur internet, parce que ce n'est pas sérieux. Ce n'est pas parce que l'on est sur Internet que l'on ne doit pas appliquer des règles. Il faut juste trouver un bon équilibre avec le respect des droits fondamentaux. Enfin, je trouve que l'on n' a toujours pas tranché la question de la responsabilité des fournisseurs d'accès. Cela fait des années que j'attends.

Myriam QUEMENER

Je tiens vraiment à tous vous remercier. Vos interventions nous permettent d'avoir une vision complète du sujet, on voit bien qu'il y a beaucoup d'initiatives. L'ensemble des acteurs se sentent concernés, y compris les politiques qui avancent sur ces problématiques. Il reste parfois une question de moyens. Tout s'inscrit évidemment dans une dimension européenne et internationale.

Le FIC 2013
en photo

sécurité
FIC
C2013.COM
FIC 5e FORUM INTERNATIONAL CYBERSÉCURITÉ
28 et 29 Janvier 2013
Lille Grand Palais
France

GENDARMERIE
NATIONALE
GENDARMERIE
NATIONALE
CYBERCRIMINALITÉ ET
CYBERSÉCURITÉ

DARMERIE

TEOPAD. Sécurisez vos données sensibles sur smartphones et tablettes.

Magasin d'applications sécurisées

Une solution économique

Un large choix d'applications

Une solution de sécurité mobile innovante

Convivialité

Pour en savoir plus, scannez le flash code ou rendez-vous sur **thalesgroup.com/teopad** ou contactez-nous au +33 (0)1 46 13 22 29

THALES

Together • Smarter • Safer

P3 – Quelle politique industrielle en matière de cybersécurité ?

Denis FORTIER

Cette table ronde m'est chère car je suis le secteur de la politique industrielle en matière de cybersécurité depuis de nombreuses années. Différentes tables rondes ont abordé depuis hier ce point et ont permis de recueillir les points de vue d'un panel d'institutionnels et de représentants des grands industriels de la cybersécurité. Nous allons approfondir, notamment ce qui concerne la recherche et le développement.

Avant les débats, je souhaite vous présenter nos intervenants. A mes côtés, des orientations institutionnelles avec Christian Breant, de l'agence européenne de défense (AED), Pascal Chour de l'ANSSI et Guillaume Poupard de la DGA qui siègent auprès d'industriels : Vincent Marfaing, de Thalès; Jérôme Notin, de Nov'IT; Luc-François Salvador, président-directeur général de Sogeti; et Jean-Michel Orozco, de CASSIDIAN. Nous avons également le plaisir d'accueillir le sénateur Jean-Marie Bockel, qui est l'auteur d'un récent rapport sur la cyberdéfense. Je me tourne vers lui pour l'introduction du sujet.

Jean-Marie BOCKEL

Permettez-moi, tout d'abord, de remercier les organisateurs de m'avoir invité à participer à ce forum. Je voudrais aussi préciser d'emblée que c'est avec beaucoup de modestie que j'aborde ce sujet car, contrairement à la plupart des personnes présentes à cette table ronde, je ne suis pas un spécialiste de ces questions. Le point de vue que j'exprime est celui d'un homme politique qui s'est vu confier par la commission des Affaires étrangères et de la Défense du Sénat, la mission de rédiger un rapport d'information sur la cyberdéfense, dont les conclusions ont été adoptées à l'unanimité en juillet dernier. Je voudrais donc vous faire part brièvement de quelques réflexions sur la politique industrielle, avant de répondre à vos questions. Tout d'abord, pourquoi une politique industrielle en matière de cybersécurité est-elle aujourd'hui nécessaire ? À mes yeux, il est crucial pour notre pays de conserver une autonomie stratégique dans un domaine qui joue un rôle de plus en plus important dans les domaines de la défense et de la sécurité.

Afin de garantir la souveraineté des opérations stratégiques ou la sécurité de nos infrastructures

vitales, il est indispensable de s'assurer de la maîtrise de certaines technologies fondamentales, dans des domaines comme la cryptologie, l'architecture matérielle et logicielle et la production de certains équipements de sécurité ou de détection. Garder cette maîtrise, c'est protéger nos entreprises et donc les emplois des Français.
On ne doit pas négliger non plus les enjeux économiques et en matière d'emplois dans ce secteur de la défense et de la sécurité des systèmes d'information, en forte croissance, qui participe à la compétitivité d'un pays. Selon les chiffres mentionnés dans le « *plan France numérique 2020* », la contribution du numérique à l'économie française représenterait 3,7 % de l'emploi en France et contribuerait à hauteur de 5,2 % à notre PIB.
Les technologies de l'information et de la communication auraient créé 700 000 emplois en 15 ans et 450 000 emplois supplémentaires pourraient être créés d'ici à 2015.

Comment susciter et structurer une filière industrielle dans le domaine de la cybersécurité ? La France dispose d'acteurs importants avec des grandes entreprises, à l'image de Cassidian, de Thalès, de Bull, de Sogeti ou d'Alcatel-Lucent, spécialisées et renommées pour leur expertise dans les domaines de la sécurité des systèmes d'information. On trouve également en France un tissu de PME-PMI innovantes, à l'image de Prim'x et d'Arkoon en matière de logiciels et produits de sécurité ou de Sysdream, d'Atheos et de DevoTeam en matière de services. Notre pays dispose ainsi de véritables « *trésors nationaux* » dans certains domaines clés pour la défense et la sécurité des systèmes d'information. Nous avons également des savoir-faire d'excellence, par exemple en matière de cryptologie ou de cartes à puces.
Toutefois, le secteur des fournisseurs français de solutions en sécurité des systèmes d'information souffre aujourd'hui de plusieurs lacunes :
- une trop grande fragmentation qui entraîne une concurrence destructrice entre les entreprises françaises et entrave le développement des PME ;
- une difficulté d'accès à la commande publique et un problème majeur d'accès au financement pour les PME, même si divers mécanismes existent comme celui des investissements d'avenir;
- un positionnement trop « *franco-français* » pour assurer le développement de groupes solides, exporter et gagner des parts de marché à l'étranger ou nouer des partenariats à l'échelle internationale ou mondiale.
Si le marché mondial est aujourd'hui dominé par des sociétés américaines, israéliennes, chinoises, russes et indiennes, la France pourrait, si elle en a la volonté, éventuellement en partenariat avec d'autres pays européens, développer une industrie complète et souveraine dans le domaine de la sécurité des systèmes d'information, à la fois dans les secteurs des matériels, des logiciels et des services.
Il n'est pas encore trop tard mais il faut s'y engager ! Je plaide donc, dans mon rapport, pour une politique industrielle volontariste, afin de soutenir le tissu industriel des entreprises françaises, notamment des PME, proposant des produits ou des services importants pour la sécurité informatique. De même qu'il existe en France une base industrielle et technologique de défense (BITD), je considère qu'il devrait exister une base industrielle et technologique en matière cyber. Il s'agit là, à mes yeux, d'un dossier qui devrait être érigé comme une priorité dans le cadre du Livre blanc sur la défense et la sécurité nationale, du séminaire gouvernemental et de la feuille de route pour le numérique que le Gouvernement devrait publier en février prochain.

Qu'en est-il hors de nos frontières ? Comme j'ai pu le constater lors de mes déplacements à l'étranger, en France, le partenariat avec le secteur privé en matière de cybersécurité est beaucoup moins développé qu'aux Etats-Unis, au Royaume-Uni ou en Allemagne. Les autorités américaines ont engagé depuis déjà plusieurs années une étroite coopération avec le secteur privé. La Conférence RSA réunit ainsi tous les ans la plupart des acteurs, tant publics que privés, de la cybersécurité aux Etats-Unis. Le Pentagone coopère étroitement avec les entreprises américaines du secteur de la défense, mais aussi des sociétés de services, telles que Cisco et Symantec. En 2007, le département américain de la Défense a lancé un programme de cybersécurité et de protection de l'information de la base industrielle de défense.
Ce programme, basé sur le volontariat, est destiné aux entreprises du secteur de la défense et consiste à échanger des informations techniques et opérationnelles sur les menaces. Il réunit actuellement une quarantaine d'entreprises et devrait être étendu à l'ensemble des sous-traitants du secteur de la défense. Ce programme a permis de mieux comprendre les attentes des entreprises, de renforcer la confiance et de mettre en place une collaboration étroite entre secteur public et secteur privé.
La stratégie britannique de cybersécurité met également l'accent sur les relations avec le secteur privé. Cette réflexion s'inscrit dans le cadre des efforts du Gouvernement pour développer ses relations avec le secteur privé et, pour sensibiliser davantage à la menace que représente la cybercriminalité. Il y a un an, le Premier ministre M. David Cameron a ainsi réuni les dirigeants d'entreprises appartenant à des secteurs d'activités d'importance vitale pour évoquer avec eux les questions liées aux cybermenaces.

Enfin, en Allemagne, des relations étroites existent entre le gouvernement et l'agence chargée de la protection des systèmes d'information, le BSI, avec les industriels du secteur, notamment en matière de normalisation.

Quel pourrait être le rôle de l'État ? En France, l'État se positionne est trop souvent régulateur ou contrôleur et pas assez partenaire. Il faut bâtir un partenariat autour d'industriels et de prestataires de service de confiance. Les entreprises attendent davantage d'échanges avec l'État. On pourrait à cet égard s'inspirer du programme lancé par le département de la défense aux Etats-Unis ou du *cyber hub* britannique, pour renforcer les échanges entre l'État et les entreprises du secteur de la sécurité des systèmes d'information.
L'État doit aussi encourager une consolidation structurelle et capitalistique du secteur, en favorisant le maintien ou l'émergence de « *champions* » nationaux ou européens. A cet égard, on peut mentionner le cas préoccupant d'Alcatel-Lucent qui mériterait, une attention particulière de la part de l'État, compte tenu des enjeux, non seulement économiques et d'emplois, mais aussi en termes de souveraineté. Enfin, notre dispositif de financement public de la recherche-développement ce doit d'être renforcé et clarifié.

Quel rôle pourrait jouer l'Union européenne ? Si la protection des systèmes d'information doit demeurer avant tout une compétence nationale, car elle touche directement à la souveraineté de chaque État, l'Union européenne joue un rôle important à jouer car une grande partie des normes relèvent de ses compétences. Il me semble donc indispensable que l'Union européenne se dote d'une véritable stratégie européenne qui englobe l'ensemble des questions

liées au cyberespace, dont les aspects industriels. La Commission européenne devrait d'ailleurs présenter prochainement une communication sur ce sujet. L'Europe pourrait également être plus ambitieuse et avoir la volonté, comme d'autres puissances émergentes, de parvenir à une souveraineté numérique, ce qui veut dire retrouver la maîtrise de certains composants (comme les microprocesseurs par exemple). Aucun état membre ne peut atteindre seul cette souveraineté. L'Europe seule le peut. Je plaide donc pour une véritable politique industrielle à l'échelle européenne et un partenariat entre les entreprises françaises et européennes, par exemple dans le domaine sensible des équipements de cœur de réseau. Enfin, je pense utile d'insister sur le rôle de l'État en matière de formation et de sensibilisation. Il existe aujourd'hui peu d'ingénieurs spécialisés dans la protection des systèmes d'information et les entreprises ont du mal à en recruter.
Il y aurait quatre à cinq fois plus d'offres d'emplois disponibles que d'ingénieurs spécialement formés à la sécurité informatique. Nous devrions mettre l'accent sur la formation et développer les liens avec les universités et les centres de recherche. Il me paraît également nécessaire de sensibiliser des utilisateurs, afin de promouvoir une *hygiène informatique* élémentaire, pour reprendre l'expression du directeur général de l'ANSSI, Patrick Pailloux.

Denis FORTIER

Merci monsieur le sénateur. Jean-Michel Orozco, nous venons d'entendre un plaidoyer visant le monde de l'industrie et des services. Comment vous réagissez vous en qualité de PDG de Cassidian CyberSecurity ?

Jean-Michel OROZCO

En ce qui concerne la politique industrielle en France ou en Europe, je rebondis sur ce qui vient d'être dit, il faut savoir concilier à la fois les souverainetés nationales et la nécessité d'aborder un marché plus large qu'un marché strictement national. Si on veut être efficace, il faut être capable de concilier les besoins de souveraineté et la capacité d'investissement des industries. Pour revenir sur le problème de la politique industrielle et les relations entre l'État et l'industrie, une première remarque s'impose : la politique industrielle appelle des financements et des investissements concernant de nombreux secteurs. Je pense qu'il y a un investissement à faire au niveau étatique et industriel. Auquel chacun doit contribuer. Cet investissement, doit déjà cibler l'établissement et le développement d'une filière technologique nationale et probablement européenne. Si l'on veut des technologies et des solutions économiquement viables, il est important d'avoir un accès à un marché le plus large possible. Évidemment, il faut concilier cette ouverture avec les enjeux de la souveraineté nationale. Cassidian sait bien le faire. Le deuxième volet d'investissement doit porter sur la formation. Actuellement, il existe un vrai problème de pénurie de ressources. Les formations ne sont pas structurées, très peu d'étudiants sortant des écoles sont correctement formés. Plusieurs initiatives ont été lancées en France. En ce qui concerne, nous avons organisé une coopération avec Télécom Sud Paris de façon à mettre en place l'équivalent d'un master spécialisé à la rentrée 2013. Cette initiative sera bénéfique pour l'ensemble des industriels et des organismes étatiques en France.

Denis FORTIER

Vous rejoignez le sénateur Bockel sur ce constat du déficit de formation et du manque d'étudiants spécialisés.

Jean-Michel OROZCO

La cybermenace est une menace létale pour nos sociétés occidentales. Elle est également extrêmement asymétrique. On parle bien d'un enjeu de souveraineté au sens de la sécurité d'une nation, que ce soit la nation française ou les nations européennes, les nations occidentales. Il faut que les industries et les Etats prennent la mesure de cet enjeu de sécurité majeure. Cela signifie des investissements significatifs de la part de l'État sur le plan de R&D pour mettre en place une véritable politique industrielle. Les industriels ne peuvent assumer seuls cet effort.
Je ne critique la position de l'État et ses actions car elles sont déjà très positives. A titre d'exemple, l'ANSSI a mis en place beaucoup de choses dans les années passées. Beaucoup d'avancées se font dans ce contexte-là, mais il faut aller plus loin, plus vite et plus fort. Les États-Unis sont beaucoup plus structurés que nous. Ils ont un marché plus large et ils ont aussi une prise de conscience antérieure. Ils ont commencé à se poser des questions, sur la manière de contrer la menace chinoise. La plupart des industriels américains font plus d'un milliard de dollars de chiffre d'affaires dans le domaine, que ce soit Boeing, Lockheed Martin ou Northrop Grumman. C'est également vrai pour les grands fournisseurs de solutions, comme McAfee ou Symantec. Si l'on compare la situation européenne en matière de structuration par rapport à la posture américaine, pour revenir notamment sur ce que disait la ministre Fleur PELLERIN hier, on constate une fragmentation extrême en France et, d'une manière générale, en Europe. Les acteurs européens, quels qu'ils soient, n'ont pas atteint la masse critique par rapport aux grands acteurs américains, quel que soit le positionnement dans la chaine de valeur. Il n'a pas une politique de R&D suffisamment efficace, pour le moment, dans les grands pays européens.

Denis FORTIER

Vous parlez de R&D, quel est pourcentage y consacrez-vous ?

Jean-Michel OROZCO

20% du chiffre d'affaires, ce qui est beaucoup et supérieur aux ratios de l'industrie de défense classique, qui se situe en dessous de 10%. On est sur des segments qui ont un besoin d'investissements forts en matière de R&D: c'est très clair et c'est fondamental. Il y a un point sur lequel je voudrais attirer l'attention du public : l'investissement intéresse le niveau organisationnel, c'est-à-dire au sens des processus, des relations États/industries, de la création de cercles de confiance au niveau national mais également européen, avec des degrés de confiance qui doivent être adaptés en fonction des frontières que l'on franchit. Cette relation États/industries est fondamentale. Elle est déjà en place en France et en Royaume-Uni. Nous faisons partie, en ce qui nous concerne, du cercle national en France, en Grande-Bretagne et en Allemagne. Mais nous manquons encore de cercles de confiance inter-européens.
Enfin, je crois qu'il faut investir dans la régulation. Il y a des cultures différentes au niveau européen. On ne parle pas de la même façon de régulation en France, au Royaume-Uni ou en Allemagne. Pour arriver à mettre en sécurité la nation fran-

çaise, il faut passer probablement par un minimum de moyens coercitifs en matière de régulation. Les choses ne viendront pas naturellement par elles-mêmes.
La politique industrielle nécessite un support étatique, un investissement industriel, dans la formation, les processus organisationnels et une régulation.

Denis FORTIER

Je vais laisser la parole à Vincent Marfaing, vice-président de la Business Line Sécurité des Technologies de l'information chez Thalès. Partagez-vous ce constat sur cette problématique de l'investissement dans ses multiples facettes ?

Vincent MARFAING

Je le partage mais je vais essayer d'en donner une illustration au travers des activités industrielles proprement dites. Le mot « *industriel* » a été beaucoup utilisé ce matin mais de quel industriel parle-t-on ? Celui qui fournit des prestations de sécurité, ou s'agit-il d'un industriel qui va fournir un système de contrôle du trafic aérien, une station de commande du système Galileo ? Finalement, lequel des deux est en charge de la sécurité du système opéré ? Je constate, dans les échanges d'hier et aujourd'hui, que nos solutions de sécurité sont perçues comme un complément « *après coup* » relativement ingéniérique par rapport aux systèmes renforcés.
Le point de vue de Thalès ou le point de vue industriel en général, est que les deux compétences , de l'industriel de sécurité et de celui qui fournit l'applicatif, sont nécessaires pour renforcer au niveau du design, ce que l'on appelle la cybersécurité « *by design* », la robustesse de nos systèmes. Au-delà du fait que cela ait l'air créatif, c'est une nécessité de s'y préparer à l'avance sachant que l'on traite des systèmes à très longue durée de vie. C'est une nécessité impérieuse car les menaces les plus sophistiquées sont celles qui tirent profit de la connaissance de l'architecture, des mécanismes, des protocoles de ces systèmes là. Stuxnet avait la connaissance des centrifugeuses Siemens et cela a contribué à la sophistication de l'impact et qui nécessite finalement la prise en compte de la sécurité en amont.
Pour revenir sur la problématique de l'investissement, je voudrais également rebondir sur les propos de Jean-Michel Orozco, avec une illustration complémentaire. Un industriel, tel que Thalès ou Cassidian, faisant face à un cahier des charges pour des systèmes applicatifs, va souvent trouver des « *requirements*[2] » assez vagues, voire absents, sur la protection des systèmes. Dans un contexte de compétition intense, la tentation est grande de minimiser la portée de ce que l'on va fournir dans cette catégorie, d'où la nécessité non seulement d'élever la prise de conscience de nos clients et, en particulier, au niveau des infrastructures vitales, comme on le fait aujourd'hui. C'est un débat utile quant à l'obtention d'un minimum réglementaire pour assurer à la fois la protection de nos systèmes vitaux mais également une élévation de ce que j'appelle le nivèlement par le bas de la fourniture de nos industriels.
La lourdeur des investissements nécessite une forme de coopération et même un investissement commun entre industriels et l'administration. Je pense à des spécifications, à des concepts généraux et même au besoin d'une direction, d'une feuille de route. Aujourd'hui on parle de « *mettre de l'argent* », mais pourquoi faire ?

1 - Test d'intrusion visant à simuler une attaque. On analyse alors les risques d'une mauvaise c configuration, les défauts de programmation ou encore d'une vulnérabilité liée à la solution testée.

2 - C'est une déclaration qui identifie un attribut nécessaire, la capacité, la caractéristique, ou la qualité d'un système pour obtenir la valeur et l'utilité

Cette feuille de route doit se construire entre nous comme on le fait aujourd'hui et doit nous guider pour en faire le retour le plus utile.

Denis FORTIER

En matière de recherche et développement, un ratio de 20% a été cité. De quel ordre est-il chez Thalès ?

Vincent MARFAING

Les ratios sont similaires. Notre challenge n'est pas d'en faire plus ou moins mais de le faire de la manière la plus utile au sens de la coopération que j'ai évoquée. Ceci nécessite finalement la délimitation d'un cercle de confiance, qui est une notion un peu floue et abstraite, mais également avec une feuille de route relative à ce que nous construisons ensemble aujourd'hui.

Denis FORTIER

Où naît l'innovation aujourd'hui ? Dans des entreprises comme les vôtres ou dans des petites entreprises que vous n'avez pas forcément identifiées ? Sur quoi porte - elle ?

Vincent MARFAING

On touche peut-être à ce que j'appelle l'image d'Épinal avec, d'une part, les petites entreprises réactives, créatives, et des grands groupes rigoureux. Je préfère utiliser des exemples concrets dans notre travail. Par exemple, sur le cloud sécurisé souverain, englobe à la fois une alliance avec Orange et Thalès mais aussi avec des petites sociétés comme Ftopia, Innovance. Cette émulsion fonctionne de manière très positive avec une innovation qui n'est pas seulement sur le conglomérat technique mais également sur le « *business model* » et la façon d'offrir nos prestations, de plus en plus en mode service déployé rapidement, qui répondent aux attentes de nos clients.

Je pense que les cycles d'innovation ne sont pas forcément les mêmes dans les grands groupes et dans les PME et la nature de l'innovation est probablement différente. Je rejoins un peu ce que vous disiez sur la partie innovation au sens service. C'est vrai que Cassidian investit beaucoup pour fournir aux industriels qui en ont besoin des services et non pas uniquement des solutions. En revanche, il est vrai que dans les petites entreprises le cycle d'innovation est beaucoup plus court. C'est une des raisons pour lesquelles nous nous intéressons à ce panorama de petites entreprises.
Cela ne veut pas dire qu'il n'y a pas d'innovation technologique dans les grands groupes. En ce qui nous concerne, nous avons des feuilles de route d'investissement. Nous ne prétendons pas détenir la vérité mais le marché est en train de se structurer. Il est encore latent mais il se structure et apparaissent de plus en plus de besoins, notamment en matière de surveillance des réseaux, d'analyse des protocoles, de ce qui se passe sur un réseau et puis, également, en terme de sécurisation des solutions de type système de production. Ce sont des secteurs dans lesquels nous investissons de façon à pouvoir apporter au marché des solutions innovantes dans des délais relativement proches.

Denis FORTIER

Monsieur le sénateur Bockel , souhaitez-vous réagir sur ce sujet ?

Jean-Marie BOCKEL

L'une de nos principales lacunes tient à la segmentation du marché et aux difficultés rencontrées par les PME en matière de financement pour accéder à la commande publique ou aux marchés à l'export. Comme j'ai pu le constater, il existe une véritable attente de la part des PME qui sont désireuses de renforcer leurs relations et leurs contacts avec l'État. Il est donc indispensable de renforcer le partenariat entre le secteur public et le secteur privé.

Denis FORTIER

Merci Monsieur le sénateur. Je donne la parole à Christian Bréant. Vous êtes directeur de la branche Recherche et Technologie de l'Agence Européenne de Défense. Tous les industriels sont présents en Europe et évidemment à l'international. Comment envisagez-vous cette recherche et comment l'Europe est-elle organisée en matière de recherche et développement dans ce domaine ?

Christian BREANT

Tout d'abord, un mot pour rappeler que l'Agence Européenne de Défense est là pour préparer les capacités opérationnelles des États membres.

Denis FORTIER

Combien de personnes travaillent pour une agence comme la vôtre ?

Christian BREANT

120 personnes sont basées à Bruxelles et travaillent au profit des 27 pays membres. Nous avons un budget de fonctionnement voté chaque année par les États membres. Tous les projets sont alors décidés sur des budgets *ad hoc*, ce qui veut dire que, pour chaque projet, une décision spécifique est adoptée par les États contributeurs. Cela commence à deux pays et peut monter jusqu'à 27. Majoritairement, les projets concernent 5 à 8 pays en moyenne, dans des géométries très variables. Les projets R&T dont j'ai la charge, atteignent en moyenne quelques millions d'euros, et peuvent aller, pour les plus ambitieux, à une cinquantaine de millions d'euros, lorsqu'il s'agit de démonstrateur technologique comme le projet MIDCAS « *voir et éviter* » que l'on conduit dans le domaine de l'insertion des drones dans la circulation aérienne civile.

Denis FORTIER

De quand datent les premiers programmes sur le cyber que vous avez traités par l'Agence européenne ?

Christian BREANT

Cela très récent du fait, que la cyberdéfense n'a réellement été approuvée par les États membres, comme une priorité, que l'année dernière. Jusqu'à l'année dernière, les États membres ne souhaitaient pas coopérer dans le domaine de la cyberdéfense. Nous sommes vraiment dans les premières étapes. Une équipe projet a été mise en place pour pouvoir discuter de ces thématiques au sein des pays. Assez vite une vingtaine de pays sont devenus partenaires, ce qui montre bien que c'est un sujet d'intérêt.
Il faut aussi noter le caractère fortement dual de la cybersécurité. Nous avons donc été naturellement associés, à l'élaboration de la stratégie européenne dans le domaine de la cybersécurité entre la Commission et le Conseil. Et il est impor-

tant de noter que, non seulement l'ensemble des directions générales de la Commission ont été impliquées, mais également le Conseil, c'est-à-dire le Service Européen d'Action extérieure et l'Agence Européenne de Défense, Madame Ashton étant à la fois vice-présidente de la Commission mais aussi Haute Représentante pour les Affaires étrangères et la Défense.
Nous avons d'excellentes relations avec la Commission mais aussi avec les autres agences, comme l'ENISA, qui offrent un excellent effet de levier pour les États membres. Nous avons aussi récemment été associés au Centre européen de lutte contre la cybercriminalité (EC3) avec lequel nous allons coopérer de plus en plus. L'EC3 mobilise actuellement entre 40 à 50 personnes et pourrait compter d'ici deux ans une centaine de personnes. Ce centre vient juste de se mettre en place. Il faudra identifier les domaines pour lesquels un travail commun sera possible. Je souhaiterais aussi indiquer que l'on développe de plus en plus de coopération avec la Commission dans le domaine de la sécurité, le domaine de la cybersécurité étant bien sûr beaucoup plus large, car impliquant un grand nombre de directions générales.

Nous avons lancé de notre côté une première étude sur l'identification des priorités technologiques sur lesquelles les pays veulent coopérer en matière de cyberdéfense. En parallèle, la Commission a fait la même démarche dans le domaine du cybercrime. L'idée est de faire des actions complémentaires et de pouvoir échanger nos résultats par la suite. Nous avons d'ailleurs organisé en octobre 2012, conjointement entre la Commission et l'Agence, un workshop dans ce domaine. L'idée est bien de le poursuivre, à l'horizon 2020, qui représente une nouvelle préparation du programme de coopération européen dans le domaine de recherche qui intègre les concepts liés à la sécurité et à la défense. Beaucoup de technologies sont communes. Nous allons regarder de manière plus large dans d'autres domaines comme les technologies de l'information, de la communication, ce que la Commission appelle les technologies clés (*key enabling technologies*), qui offrent de nombreux domaines dans lesquels on pourrait travailler en commun.
Pour vous donner une idée du niveau de coopération actuel, dans les cinq dernières années, les États ont investi environ 700 millions d'euros de recherche à travers l'Agence européenne de Défense. C'est à la fois peu, parce que cela ne représente au niveau européen que 10% de leur coopération, mais c'est quand même la concrétisation de la volonté de travailler de plus en plus avec l'Agence, et dans des formats très variables. Évidemment, notre enjeu est aussi de travailler étroitement avec la base industrielle de défense et je voudrais terminer par ce point là. Il s'agit des « *non-dépendances* » technologiques. J'estime que, non seulement on doit traiter ce sujet pour les technologies de défense mais aussi, d'une manière générale en Europe, pour toutes les technologies stratégiques. Je pense que la cybersécurité en est une. Les composants, les logiciels qui sont développés en Inde, les réalisations qui peuvent être faites partout dans le monde, y compris à partir de terres rares (que la Chine détient en grande majorité) donnent un haut niveau de dépendance technologique et nous devons bien analyser quels sont vraiment les domaines sur lesquels l'Europe souhaite pouvoir garder une certaine non-dépendance. Je ne parle pas d'indépendance parce que nous n'en avons certainement pas les moyens, mais je dirais une certaine non-dépendance dans certains domaines clés de manière à être réellement en mesure de pouvoir bien les maîtriser.

Denis FORTIER

Pensez qu'il y a une vision partagée de l'ensemble des États membres. Peut-on dire qu'il y a une Europe de la cybersécurité au sens industriel ? Quels en sont les pays leaders ?

Christian BREANT

Non, je ne le crois pas, il faut être raisonnable. Il existe quelques pays leaders mais aujourd'hui nous rencontrons des problèmes de confiance mutuelle et toute cette problématique de non-dépendance touche évidemment à un autre sujet très sensible qui est la sécurité et l'approvisionnement. Bien sûr, si les technologies sont développées dans d'autres pays, y compris européens, on peut en assurer le contrôle mais nous ne sommes pas à l'abri d'une prise de capital ou de contrôle de certaines entreprises dans d'autres pays et de ne plus disposer des mêmes outils pour effectivement assurer la maîtrise de la base industrielle.

Jean-Marie BOCKEL

Dans mon rapport, je souligne tout l'intérêt de renforcer la coopération bilatérale avec l'Allemagne et le Royaume-Uni. En effet, dans un domaine comme la cybersécurité, qui repose sur la confiance, il est très difficile de coopérer à vingt-sept et la coopération bilatérale est souvent plus efficace.
La cyberdéfense fait d'ailleurs partie des domaines de coopération des accords franco-britanniques de défense de 2010. De même, la coopération avec l'Allemagne est très étroite, notamment entre l'ANSSI et son homologue allemand, le BSI. L'expertise de l'ANSSI est reconnue par nos principaux partenaires et il existe une véritable attente pour renforcer notre coopération dans ce domaine. Je pense notamment aux aspects industriels où nous aurions intérêt à nous rapprocher de nos partenaires allemands. Il ne faut non plus négliger également la place de certains petits pays, à l'image de l'Estonie, qui sont très en pointe sur le sujet, pour des raisons évidentes, et qui sont très désireux de nouer des relations avec la France dans ce domaine, auprès de l'agence nationale de cybersécurité estonienne.
Toutefois, au sein de l'Union européenne, comme de l'OTAN, un grand nombre de États membre ne sont pas encore suffisamment sensibilisés à ces questions. Or, dans la chaîne de cyberdéfense, la sécurité de tous repose généralement sur le maillon le plus faible.

Denis FORTIER

Vincent Marfaing, avez-vous un exemple ?

Vincent MARFAING

Oui, je voulais juste citer un exemple pour illustrer une coopération dans le domaine de la sécurité qui fonctionne. l'OTAN comporte un ressort économique, un ressort opérationnel puisqu'en opération les pays doivent coopérer aujourd'hui. Il faut savoir qu'il y a un catalogue de produits de sécurité qui existe et qui est partagé. Il se trouve que certains fournisseurs, c'est le cas de Thalès, produisent des produits sécurisés qui sont achetés par 25, 27 pays simultanément et utilisés en opération. C'est un cas de réussite.

Denis FORTIER

Merci. Je vais céder la parole à Guillaume Poupard,est ingénieur en chef de l'armement à la Direction générale de l'Armement du

Ministère de la Défense. Comment vous réagissez par rapport aux perspectives européennes ?

Guillaume POUPARD

Nous avons des relations mais je voudrais avant tout revenir sur les questions de souveraineté dont nous n'avons toujours pas citées. Pourquoi a ton besoin de souveraineté? C'est vrai que cela peut paraître choquant de ne pas partager. et l'on irait plus vite, en mettant en commun nos différents budgets. Si l'on creuse le sujet jusqu'au bout, nous arrivons à la question essentielle de la protection de nos secrets, même si cela peut appraître très rétrograde de le formuler ainsi. Notre position est que, pour être une nation influente, il faut être capable de protéger ses secrets militaires, étatiques, nos secrets liés au patrimoine scientifique et technique. Cette capacité rend crédible vis-à-vis de nos grands partenaires. Ce n'est pas une invention franco-française, ce ne sont pas les militaires qui disent ça dans leur coin, mais nos partenaires. Si vous voulez que nous allions en opération avec vous, si vous voulez que nous échangions des choses très sensibles et que nous ayons besoin d'échanger pour être efficace, il faut que vous soyez capable de protéger vos secrets. Le déroulement de cette logique débouche sur le besoin de faire des produits de chiffrement, ce que nous faisons depuis très longtemps en France. Très peu de pays au monde font leur propre chiffrement. On a un long partenariat avec Thalès dans ce domaine là. Nous disposons aujourd'hui de personnes qui sont capables de tout concevoir depuis les algorithmes cryptographiques que nous faisons avec l'ANSSI, jusqu'aux composants de sécurité. Très peu de pays au monde qui détiennent ce potentiel et notre ambition est de rester dans ce peloton de tête et d'être capable d'être indépendant.

Le paradoxe est de vouloir être souverain, indépendant sur certains sujets de manière à pouvoir coopérer avec nos partenaires. Ceci étant dit, il y a d'autres domaines où l'on peut tout à fait coopérer au niveau européen. Au sein du ministère de la Défense, nous sommes plus tourné vers l'OTAN . Cette coopération se fait au travers d'aspects un peu plus réglementaires. On réfléchit ensemble pour mettre en œuvre de la sécurité, au sens large, au sein de nos réseaux. Nous nous appuyons sur une base industrielle de défense qui est essentielle et représentée ici par les grands maîtres d'œuvre qui savent à la fois se refermer au niveau national, quand il y a un fort besoin de souveraineté, et s'ouvrir parce qu'ils ont en général plusieurs pieds dans les pays les plus influents en matière de défense.

Denis FORTIER

Nous avons entendu tout à l'heure divers point de vue sur le financement de la R&D, qui sont d'ailleurs relativement convergents. Comment la DGA agit-elle?

Guillaume POUPARD

Nous avons, en effet, au sein du ministère de la Défense un rôle de financement, plus généralement de pilotage. Nous ne sommes pas uniquement des banquiers. Dans tous les domaines, nous confions des études « *amonts* », c'est-à-dire des travaux de recherche à des industriels, en général nationaux voire internationaux, mais en privilégiant le développement de la base industrielle. Pour vous donner une idée, en ce qui concerne la cybersécurité, cela se chiffrerait jusqu'à présent à environ 10 millions par an, ce qui est à la fois beaucoup et peu. Peu, peut-être, à l'échelle du besoin mais beau-

coup si le but est réellement d'employer cet argent, qui est quand même de l'argent public, à bon escient.

Denis FORTIER

C'est vous qui établissez les programmes dans lesquels ces 10 millions vont être distillés, si je puis dire ?

Guillaume POUPARD

Exactement, donc on définit les sujets techniques, on passe les contrats.

Denis FORTIER

Quels sont les sujets ? Sauf si cela confidentiel.

Guillaume POUPARD

Il y a des choses confidentielles mais tout ne l'est pas. Typiquement, on sépare les questions liées à la protection, c'est-à-dire ce que l'on a appelé la sécurité des systèmes d'informations et qui est dans une certaine mesure l'héritière du chiffre. On se pose toujours des questions pour savoir comment faire de bons chiffreurs, comment bien protéger l'information en stockage et en communication, ce qui constitue l'aspect *protection*. L'incrémentation de cela et de manière propre dans des équipements qui sont robustes n'est pas du tout résolue. Il faut suivre les technologies. Aujourd'hui, nous nous intéressions à faire des chiffreurs à 100 gigabits par seconde, ce qui est beaucoup pour du hardware ou des logiciels. On a des travaux permanents à conduire là-dessus. On a des travaux sur les aspects de la cyberdéfense au sens de la surveillance des réseaux et des réactions. Cela concerne le développement de sondes innovantes qui vont prendre les attaques à contre-pied en détectant des attaques originales. Des travaux intéressent également tout ce qui est supervision de sécurité. Il faut bien voir in fine que toutes ces informations remontent, sont agrégées au sein de sondes de supervision qui sont gérées par des militaires et des civils détenant certaines compétences. Tout n'est pas résolu aujourd'hui sur la manière de présenter l'information et d'aider ces auteurs à réagir de manière efficace. L'expérience que l'on a des crises passées, qui sont heureusement en France des petites crises, c'est que, très souvent, les gens n'étaient pas prêts à réagir et ont perdu énormément de temps. Dans le domaine de la cyberdéfense, le temps, ce n'est peut-être pas de l'argent, mais c'est quelque chose d'absolument essentiel pour être efficace.

Avant, nous nous intéressions typiquement aux systèmes d'information et de communication car c'était la base de notre métier. De plus en plus, la question des systèmes d'arme se pose puisque nous avons beaucoup de technologies qui viennent irriguer les systèmes d'arme, et c'est ce qui fait aujourd'hui leur efficacité. Il faut être capable de sécuriser les systèmes d'arme avec des contraintes qui ne sont pas celles des réseaux informatiques : j'ai l'habitude de dire qu'un hélicoptère de combat c'est un système d'arme avec un rotor mais ça pose évidemment des contraintes…

Denis FORTIER

Un conférencier précisait hier qu'il y avait sans doute une prise de risque assez importante lorsqu'on prend pour raisons économiques, des solutions sur étagère au détriment de solutions peut-être propriétaires, différentes ou uniques. Quel est votre point de vue sur cette question ?

Guillaume POUPARD

C'est vraiment le cœur de la réflexion. Nous ne pouvons pas recréer des arsenaux. En France, nous n'en avons pas les moyens, et même si cela était le cas je ne sais pas si l'on y arriverait. Il faut bien voir que la technologie est mondialisée et que, dans des domaines d'expertise, il y a souvent avoir un acteur mondial. Je pense à la téléphonie, qui intéresse beaucoup d'acteurs mais, in fine, quand on regarde vraiment qui a la maîtrise, qui fait l'implémentation de tel protocole, de tel système, il y a très très peu d'acteurs.
En revanche, notre démarche, qui est directement liée, d'ailleurs, à la politique industrielle, est vraiment une démarche d'architecture. On peut l'appeler « *sécurité by design* ». Comme monsieur Jourdain, nous en faisons depuis longtemps sans véritablement le savoir. Cette idée d'architecture est essentielle puisqu'elle permet de dire dire que l'on va penser dès le départ nos systèmes en fonction des impératifs de sécurité. Ce n'est pas la peine de concevoir des systèmes que l'on ne saura pas ensuite réaliser dans de bonnes conditions et ce n'est pas la peine de s'imaginer que l'on va pouvoir apporter la sécurité après. Prenons un hélicoptère de combat: peut-on le fabriquer et se poser ensuite la question de sa sécurisation ? C'est totalement illusoire. Nous travaillons sur l'architecture, pour ensuite poser des briques naturelles à développer et le partage se fait pour des raisons de sécurité. Il y a des choses que l'on fait en interne « *étatique* », notamment les algorithmes cryptographiques parce que cela demeure plus efficace. Nous le faisons avec l'ANSSI. La réalisation se fait parfois sur co-développement avec des industriels. Cela est plus osé parce que l'on mélange des étatiques et des industriels pour travailler ensemble. Il y a des gens ici qui font cela avec nous et parfois nous faisons appel à des briques qui viennent de logiciels libres. Vous voyez que tout est assez ouvert, c'est une vaste palette et c'est l'objectif. On ne veut se priver d'aucune source d'approvisionnement. Il y a une forme d'opportunité. La dernière brique c'est vraiment les PME que l'on soutient.

Denis FORTIER

Comment sélectionnez-vous ces PME ?

Guillaume POUPARD

Nous les connaissons et travaillons en commun avec l'ANSSI qui en a recensé 400 en France dans le domaine. Certaines sont très intéressantes. Nous dialoguons, essayons d'avoir des marchés étatiques un peu unifiés pour les aborder et pour faire une sorte de catalogue.

Denis FORTIER

Merci. Monsieur le sénateur, vous vouliez ajouter quelque chose sur ce sujet ?

Jean-Marie BOCKEL

Ce que dit Guillaume Poupard montre bien l'importance majeure du rôle de la DGA sur ces questions. C'est la raison pour laquelle j'ai préconisé dans mon rapport un renforcement de vos moyens, y compris humains, sur lesquels nous avons eu des réponses du gouvernement. Le ministre pourra le confirmer et c'est la richesse humaine qui, en l'occurrence, a une grande valeur.

Il y aussi la question sensible des aspects offensifs. Cette question est évoquée dans le Livre blanc de 2008 mais toutes ses implications

ne sont pas encore clarifiées. Comment identifier l'auteur d'une attaque informatique ? Les mesures de rétorsion doivent-elles se limiter aux moyens informatiques ou bien peut-on envisager également des moyens conventionnels ? Il faudra que nos experts trouvent des réponses à ces questions. Dans mon rapport d'information, je m'interroge sur l'élaboration d'une réflexion et d'une doctrine publique sur les moyens offensifs.

La découverte en 2010 du programme malveillant Stuxnet a ouvert la « *boîte de pandore* » de l'utilisation par des États ou des organisations d'attaques informatiques à des fins de destruction. Selon les révélations du journaliste américain David Sanger, Stuxnet aurait été conçu par les Etats-Unis et Israël pour retarder le programme nucléaire militaire iranien et aurait détruit un millier de centrifugeuses de la centrale nucléaire iranienne de Natanz. Mais on imagine les dégâts que pourrait causer un tel programme malveillant s'il était utilisé à l'encontre de nos infrastructures d'importance vitale, comme l'énergie, les transports ou la santé.

Denis FORTIER

Luc-François Salvador, quel est votre réponse en tant qu'industriel dans le domaine de la cybersécurité ?

Luc-François SALVADOR

Je crois que le sujet a été fouillé sous plusieurs angles. Je voudrais mettre en avant un point de perplexité : où est l'argent ? L'État recherche des technologies très avancées avec des aspects de ruptures alors que le «civil» cherche des technologies éprouvées avec des innovations évolutives. Nous sommes à la rencontre de ces deux mondes et les marchés ne sont pas aussi clairs qu'on peut le dire. Nous savons grands équipementiers. Quand on regarde leur couverture du marché aujourd'hui, ils sont assez équilibrés. En revanche, une fois que l'on a quitté les États-Unis, notamment en Europe, ces marchés sont très fragmentés et cela pose la question de l'affectation des ressources financières lorsque l'on veut définir une vraie politique industrielle. En France l'État a bien avancé. Quand on regarde l'évaluation des forces et notamment des ressources dont l'État s'est doté entre l'ANSSI, la DGA et ceux que l'on n'a pas le droit de nommer, entre 1200 à 1500 grandes compétences ont été mobilisées. Si vous regardez les chiffres que les États-Unis donnent tout récemment, ils portent sur environ 4 900 ressources mais on ne sait pas lesquelles.

Denis FORTIER

Tout le monde n'est pas d'accord avec cette vision. J'ai entendu des discours inverses disant que l'État n'avait plus les moyens et donc que les grandes compétences partaient.

Luc-François SALVADOR

Je possède des preuve à ce sujet; un des soucis est la formation c'est-à-dire la production de la ressource. Il y a des initiatives intéressantes, la chaire de l'IHEDN, celle de Thalès et de Sogeti avec Saint-Cyr et, en matière de chiffrement, nous avons parmi les plus belles écoles au monde. Les Coréens, les Israéliens, les Américains le savent et ils viennent les voir, preuve que l'Etat agit. En matière de politique industrielle, des choses ont été faites dans le régulatoire et le normatif et il faut continuer. Il faut notamment endurcir les systèmes, durcir les règlements, notamment le régime des grands sous-traitants

auprès de l'État où des entreprises dites souveraines puisqu'il subsiste des états de déshérences qui ne sont pas acceptables. Il faudrait aussi réfléchir juridiquement à renforcer ce qu'est la notion d'opérateur de confiance qui existe en terme de concept mais qui n'est pas établi sur des pages juridiques fortes et formelles.

Denis FORTIER

De votre point de vue, ce cercle de confiance mériterait d'être établi de manière plus formelle ?

Luc-François SALVADOR

Ah oui! Absolument, au moins juridiquement.

Denis FORTIER

Comment fait-on cela ?

Luc-François SALVADOR

Il existe certains outils notamment quand vous travaillez dans des domaines « *critiques* » de l'État. Vous ne pouvez pas courir le risque, lors d'un grand marché mis en avant par l'État, qu'un opérateur, qui ne serait pas de confiance, ne soit pas traité équitablement et aille se plaindre devant un tribunal. Pudiquement, Jean-Marie Bockel l'a dit et ces sujets existent notamment chez certaines nationalités d'équipementiers. Un dernier point n'a pas été soulevé dans le débat qui est la promotion de ce qu'est l'équipe « *France* » en matière de politique industrielle parce que ces sujets de cybermenaces sont en train de monter un peu partout. Des pays du Moyen-Orient, d'Amérique Latine et d'Asie approchent la France pour une assistance et entretiennent des discussions. On sent bien qu'entre la DGA et l'État-major, il y a la volonté de créer ce qui pourrait être une « *dream team* » à la française qui pourrait réunir ces opérateurs de confiance et mettre en avant et promouvoir ces savoirs-faire français. C'est une opportunité à ne pas manquer. C'est quelque chose de complexe à monter. Cassidian qui agit avec Thalès, Capgemini et d'autres, plus quelques PME ce n'est pas évident. La coordination avec la DGA n'est pas non plus quelque chose de simple. Si cela réussissait on pourrait prendre des positions majeures au Moyen-Orient ou au Brésil qui est en train de se doter de forces de protection de ses plateformes pétrolières et intègre la relation cybermenace sur les processus industriels. Il en est de même en Inde, etc.

Denis FORTIER

Monsieur le sénateur, cette "dream team" ?

Jean-Marie BOCKEL

Vous n'avez pas parler de la « *Réserve citoyenne cyber* » ?

Denis FORTIER

J'en fait moi-même partie…Un mot rapidement ?

Luc-François SALVADOR

L'État-major en application du premier Livre Blanc s'est dotée d'une compétence cyber en la personne de l'Amiral Coustillière. Il a pris la décision de se doter d'une structure dite de cyber-réserve qui mobilise des représentants d'entreprises qui sont dans un engagement patriotique personnel sur les sujets de cyber. On ne constitue pas un nouveau think tank, ce

n'est pas du tout l'objet, mais en revanche on essaie de travailler sur des aspects innovants qui pourraient être demain le ciment d'une cyberforce au service de l'État.

Denis FORTIER

Pascal CHOUR, vous représentez l'ANSSI. Vous êtes responsable du bureau « *politique industrielle et assistance* ». Vous êtes en charge de la politique industrielle, mais que recouvre le terme « *d'assistance* » ?

Pascal CHOUR

Avant de parler de politique industrielle, je voudrais juste répondre ou commenter certains points sur la formation et sur le fait que l'ANSSI assécherait le marché en matière de compétences sécuritaires. Paradoxalement, j'aurai tendance à dire que c'est presque une bonne nouvelle. Évidemment, cela ne l'est pas pour ceux qui aujourd'hui cherchent ces compétences mais j'ai été enseignant-chercheur, j'ai créé il y a une douzaine d'années un master dans le domaine de la sécurité. Ces masters, ont un problème d'attractivité car ils n'attirent pas ou n'attiraient pas les jeunes ingénieurs. Je pense qu'un des problèmes était qu'ils n'y voyaient pas de filières ou d'avenir. Aujourd'hui, cette recherche de ces compétences est probablement un bon message pour les jeunes pour s'engager dans ces filières.

Denis FORTIER

Vous revenez sur le constat de la formation.

Pascal CHOUR

La formation existe si elle touche un domaine économique et si il y a des débouchés. Faire une formation qui est prévue pour 15 personnes et qui n'arrive à recruter que 10 personnes par an, montre qu'il y a un problème pour attirer les gens dans ce domaine là. Je pense qu'aujourd'hui, on est mieux parti grâce justement au message que l'on fait passer.
Pour en revenir sur la politique industrielle, on a beaucoup parlé de souveraineté voire de produits régaliens. L'ANSSI, du fait de sa position d'autorité d'agrément de ces produits s'est impliquée dans tous ces sujets depuis de plusieurs années. Je parlerais plutôt de la sécurité de tous les jours, de la sécurité qui est mis en place dans les entreprises et qui n'est pas forcément du domaine de la défense, domaine très sensible. Effectivement, l'ANSSI a orienté depuis quelques années maintenant son dispositif pour aussi s'intéresser à ce type d'entreprise. Guillaume Poupard citait effectivement l'étude que l'on a menée pour essayer d'identifier les entreprises qui font de la sécurité en France. Nous en avons trouvé pour l'instant 400. Une autre étude, l'Alliance pour la confiance numérique en a trouvé 600, même s'il y a un peu d'inflation dans ce décompte. Effectivement la première chose pour l'ANSSI c'est d'essayer de connaître l'offre qui existe sur le marché, ses forces, ses faiblesses et les secteurs orphelins, de façon à pouvoir agir sur ces secteurs lorsqu'on en a besoin. Sur la sécurité, on va évidemment essayer d'identifier les industriels. On en a de très bons, en particulier dans le domaine des composants sécurisés et de toutes les applications de ces composants. On est les leaders mondiaux sur ce sujet avec les allemands et il faut le rappeler, on a une avance technologique aussi bien en conception, en réalisation et aussi, c'est un sujet que j'aborderai un peu plus tard, en évaluation de la sécurité qui est aussi un métier de la sécurité et de la cybersécurité.

Nous allons suivre le domaine de l'édition, puisque l'on constate comme tout le monde que ce secteur est extrêmement morcelé et assez fragile. C'est un rôle de l'ANSSI d'essayer de mettre en relation des petites entreprises avec des plus grosses pour pouvoir faire des produits qui pourront trouver un marché au niveau national et au niveau international. Monsieur Salvador a parlé de la reconnaissance des opérateurs de confiance. C'est un domaine sur lequel nous sommes maintenant positionnés depuis quelques années. Un des points durs de la sécurité est de savoir ce que vaut cette sécurité. On a un dispositif, assez connu maintenant, d'évaluation et de certification de produits voire du qualificatif de produits quand il s'agit de satisfaire les besoins de l'État en matière de défense.

Denis FORTIER

Vous labellisez des produits ?

Pascal CHOUR

Nous labellisons les produits à travers des laboratoires qui sont externes à l'ANSSI mais agréés par l'Agence et dont on contrôle les compétences avec les ressources de l'Agence. Nous sommes aussi aidés par le ministère de la Défense, quand on n'a pas les compétences mais on atteint de plus en plus une autonomie en la matière. C'est un dispositif qui marche bien. Il faut savoir que la France est dans les pays en tête sur ces aspects « *évaluations* », ce qui d'ailleurs ne fait pas tout à fait plaisir à certains de nos « *grands amis* ». Cette action permet d'identifier les bons produits, ceux qui respectent un certain nombre de standards, de savoir-faire, de bonnes pratiques etc., et des référentiels qui sont d'ailleurs disponibles sur notre site en matière de cryptographie. Nous sommes également en train de la mettre en œuvre également pour les services ou les opérateurs et on essaye de qualifier des sociétés de service, des prestations de service et des opérateurs. Qualifier, c'est vérifier que ces prestataires proposent une offre qui convient à l'administration.

Denis FORTIER

Cela va donc au-delà des garanties habituelles relatives aux marchés publics.

Pascal CHOUR

En effet, l'idée est de labelliser les prestations qui offrent un bon niveau de compétences. Nous avons commencé, certains le savent probablement ici, par les prestataires d'audit en sécurité, système d'information. Nous sommes phase expérimentale. Nous allons lancer quelque chose pour identifier les prestataires dans le domaine du cloud du niveau de confiance attendu par l'ANSSI. On fera probablement aussi en 2013 quelque chose dans le domaine de la reconstruction après incident. Voilà des actions très concrètes que l'on est amené à faire. Évidemment nous nous basons base aussi sur une feuille de route qui est établie et remise à jour annuellement pour définir quels sont les secteurs qui nous faudrait accompagner pour disposer dans un temps raisonnable de produits commerciaux. Je ne parle ici que de produits commerciaux car des feuilles de route pour les produits régaliens existent déjà depuis de nombreuses années. Ces actions dans ce domaine ont déjà commencé à donner des résultats. Une autre partie de l'Agence est en lien avec les différents grands secteurs industriels : le transport, l'énergie, etc., pour essayer d'identifier ces besoins et faire en sorte de pouvoir identifier ces industriels ou des offreurs de service capables

de les proposer.

Denis FORTIER

Notre dernier intervenant est Jérôme NOTIN, président de Nov'IT. Quelles sont les prestations proposées par Nov'IT?

Jérôme NOTIN

Nov'IT aujourd'hui porte un projet qui s'appelle DAVFI, (Démonstrateur d'Antivirus Français et Internationaux). Nov'IT est une PME. L'objet de mon intervention vise à présenter par l'exemple la réussite de la mise en place d'une politique industrielle. Le consortium qui travaille sur DAVFI a obtenu des financements publics dans le cadre d'investissements d'avenir, d'appels à projet « *sécurité et résilience des réseaux* ». L'objectif est de pouvoir travailler et participer d'une manière financière aux travaux de recherche afin d'obtenir un antivirus français de confiance, fiable et maîtrisé.
Cet antivirus, pour bien naître, a bénéficié des travaux de recherche d'une personne experte en la matière qui s'appelle Éric Filiol et qui est d'ailleurs un ancien du ministère de la Défense. Éric travaille aujourd'hui au sein de l'ESIEA qui est un des membres du consortium qui porte DAVFI. La date de commencement des travaux est le 1er octobre de l'année dernière et nous avons 24 mois pour le livrer à l'État, notre financeur, avec lequel nous avons un vrai partenariat. C'est d'ailleurs quelque chose que je souhaitais signaler. Monsieur le sénateur parlait de connexions, le terme est vraiment intéressant puisque c'est ce que nous vivons au quotidien avec ce projet. Je souhaitais également parler du processus : il va y avoir de nouveaux appels à projet, j'invite donc les PME ou les plus grosses structures à se pencher sur ce dossier puisque aujourd'hui je considère que c'est un excellent moyen de financer l'innovation et à terme, de faire que des PME émergent et puissent travailler avec des grands groupes.
La mise en place de pratiques des financements d'avenir, en tout cas pour notre partie, ce n'est pas uniquement un financement public, c'est aussi un partenariat. Notre service pilote est la DGA. L'ANSSI participe également aux travaux techniques que l'on peut faire autour de l'antivirus.

GROUPE
Imprimerie Nationale

La confiance au cœur de nos identités

P4 – Le traitement judiciaire de la cybercriminalité à l'échelle européenne et internationale : quelles perspectives ?

Général Jacques HEBRARD

Nous sommes heureux de vous accueillir pour cette session de l'après-midi. Le sujet relève d'un volet judiciaire qui est important au sein du Forum international de cybersécurité. Les enjeux en matière de lutte contre la cybercriminalité sont particulièrement forts aujourd'hui. Il s'agit de lutter contre ce phénomène tout en préservant la liberté des individus, leur sécurité et celle des infrastructures étatiques et des entreprises. La délinquance organisée est aujourd'hui particulièrement active en matière de cybercrime. Elle est le fait de groupes criminels classiques qui utilisent de façon massive les nouveaux outils de communication ou abusent les technologies à commencer par celles qui font obstacle à leurs activités. Elle est aussi l'émergence de nouveaux groupes criminels tournés vers l'appropriation frauduleuse grâce aux nouvelles technologies. Le moteur de cette délinquance est évidemment le gain financier dans le contexte d'un univers numérique présentant un risque pénal moindre.
Les activités cybercriminelles franchissent souvent les frontières en une fraction de seconde et touchent plusieurs pays à la fois. Du point de vue du maintien de l'ordre, cela amène à poser les questions de la détermination de la juridiction compétente, de la loi applicable, du contrôle des frontières ainsi que de la reconnaissance des preuves électroniques. Il est évident que s'impose une coopération internationale renforcée pour combattre la cybercriminalité, car aucune action limitée à un territoire national ne saurait être efficace. Traiter cette criminalité exige une véritable harmonisation des législations pénales, l'amélioration du partage des informations, l'optimisation des moyens mis à la disposition de l'enquêteur judiciaire ainsi qu'une formation adaptée des acteurs de la chaîne pénale.
La cybercriminalité se joue des frontières. Il est impératif que les services de police et de justice coopèrent encore plus efficacement par-delà les frontières. La cadre de l'Union européenne est particulièrement favorable à cette action avec les outils très pertinents que sont les agences de coopération Europol et Eurojust et les outils de procédures communs.
La création très récente du Centre européen de lutte contre la cybercriminalité pour défendre un internet libre sûr et souverain en est une parfaite illustration. Nous allons durant cette session plénière nous intéresser aux perspectives

du traitement judiciaire de la cybercriminalité à l'échelon européen et international. Pour nous éclairer sur ce sujet, nous avons réuni cet après-midi, cinq intervenants qui vont nous apporter successivement leur expertise en la matière.
Monsieur Yves Charpenel a exercé, depuis 1976, plusieurs fonctions au siège puis au Parquet. Il a notamment exercé les fonctions de conseiller technique au cabinet du Garde des Sceaux. Il est aujourd'hui premier avocat général à la Cour de cassation.
Monsieur Quillé, directeur adjoint d'Europol, est chargé de la direction des opérations. Il a une longue expérience au sein de la Direction centrale de la police judiciaire et a occupé divers postes dans le domaine international en matière de lutte contre la criminalité organisée.
Je poursuis avec monsieur Dieudonné Tharcisse Kanyama Mbayama qui représente la magistrature de la République démocratique du Congo. Il est aujourd'hui substitut du Procureur général près de la Cour d'appel de Lubumbashi et délégué élu au Conseil supérieur de la magistrature. Il nous donnera sa vision de la problématique liée à la cybercriminalité en Afrique.
Madame Sylvie Petit-Leclair a occupé divers postes au sein de la magistrature française. Juge d'instruction, procureur, elle a exercé les fonctions de magistrat de liaison aux Pays-Bas et au Royaume-Uni. Elle nous fera part de son expérience à Eurojust puisqu'elle représente la France au sein de cette structure. Enfin, monsieur Alexander Seger représente le Conseil de l'Europe. Il est secrétaire du comité de la Convention sur la cybercriminalité.
Sans plus attendre, je vais demander à monsieur Charpenel de faire un point sur la réalité actuelle du traitement judiciaire en matière de cybercriminalité.

Yves CHARPENEL

Le traitement judiciaire de la cybercriminalité reste encore une idée neuve comme d'ailleurs le cybercrime au regard de l'historique du traitement judiciaire en général.
Le principal enjeu qui se pose au système répressif en matière de lutte contre la cybercriminalité est assez clair : comment un système judiciaire qui, en France, a été forgé au début du XIXème siècle peut aujourd'hui être capable de rendre compte, de maîtriser, de traiter un phénomène aussi nouveau, aussi diffus que celui de la cybercriminalité? Aussi loin, de la culture judiciaire ?
Pour voir quelles sont les lignes de forces des problèmes rencontrés, des perspectives, je crois qu'il ne faut pas perdre de vue que notre combat pénal, que ce soit cyber-combat ou combat classique, repose toujours sur la conjonction plus ou moins réussie, de trois facteurs incontournables. Le premier est de mobiliser des acteurs professionnels, le second de suivre des règles du jeu compréhensibles et si possible applicables, le troisième étant d'avoir des systèmes de coopération qui soient vraiment efficaces. Qui dit cybercriminalité dit nécessairement coopération et coordination, personne ne détenant les clés du coffre à lui tout seul.
Que nous révèlent de ces trois points de vue quant à la situation actuelle du traitement judiciaire de la cybercriminalité ? Chez les acteurs, il ne faut pas se le cacher, un certain désarroi. Il faut bien voir que tous les acteurs de la lutte contre la cybercriminalité en matière répressive, les magistrats, les enquêteurs, les experts, les avocats, ont été formés à des règles très différentes de l'univers du cybermonde.
D'abord, parce que le monde judiciaire et le monde pénal, sont un monde d'interprétations strictes fondées sur un droit dur, des lois présumées

intangibles. Alors qu'aujourd'hui confrontés au Cloud computing qui est exactement l'antithèse de cet univers.
Autre phénomène perturbant, le droit pénal, dans tous les pays, s'est constitué autour de l'idée qui paraissait simple de territorialité. Par définition, le cybermonde dilue à peu près complètement tout principe territorial. Face à des données aussi troublantes, il y a une sorte de chaos juridique.
Pour éviter le chaos judiciaire, les juges, en tout cas en France, ont toujours eu la même démarche. Dans un premier temps, le juge qui est un sceptique par définition, par constitution, va d'abord vers ce qu'il connaît. Cela veut dire qu'il ira moins vers ce qu'il ne connaît pas. C'est le premier constat que l'on peut fait sur la démarche des magistrats envers la cybercriminalité. Depuis la loi informatique et liberté, qui remonte tout de même à plus de 45 ans, traditionnellement les magistrats ont tenté de passer le cybermonde naissant et florissant au crible des principes traditionnels de la procédure pénale. Autrement dit, d'appliquer à des phénomènes nouveaux, des recettes anciennes.
Cela fonctionne de moins en moins. La Cour de cassation, particulièrement, joue le rôle de régulation et passe aujourd'hui ses audiences, en matière de cybercriminalité à essayer de voir comment les lois nouvelles et les pratiques nouvelles du cybermonde peuvent être réellement traitées par les principes traditionnels. A ce jeu, ce ne sont pas toujours les « *bons* » qui triomphent : nous avons ainsi l'exemple cuisant et récent de l'annulation par la Cour de cassation d'une procédure qui était née d'un faux site cyberpédopornographique réalisé par le FBI aux États-Unis qui a détecté des criminels grâce à ce « *vrai-faux* » site pédophile.
Cette procédure, en ce qui concerne les Français qui étaient concernés, a fini par être annulée tout simplement parce que l'on a appliqué non pas la facilité de la détection des criminels mais les principes fondamentaux de la procédure pénale, celui en l'espèce de la loyauté de la preuve.
Il ne faut jamais perdre à l'esprit que la simple transposition des règles judiciaires traditionnelles au cybercrime est insuffisante, la limite de l'exercice étant que les principes fondamentaux de la procédure ne sont pas solubles dans le cybermonde.
La méthode a donc montré ses limites et la seule manière de les dépasser, je crois que c'est tout l'intérêt d'une réunion comme celle-ci, c'est de renforcer la spécialisation.
Aucune autre perspective ne permettra aujourd'hui d'avancer, car finalement la cybercriminalité, toute numérique qu'elle soit, est d'abord une criminalité qui commet des dégâts et qui cause des dommages et des préjudices. Leur importance ne doit pas être sous-estimée. Tout au long de ces deux journées, vous listez les différents désordres que la cybercriminalité cause à la société, aux individus comme aux institutions. Cela montre la nécessité de ne pas céder à la tentation de privatiser les moyens d'enquêtes cybercriminels. Les enjeux fondamentaux de la nation imposent que l'État soit capable, en lien bien sûr avec le secteur privé, de mener ce combat. C'est une tentation qui est très forte et à laquelle cède un certain nombre de pays.
Nous avons besoin de magistrats et d'OPJ spécialisés et si possible regroupés dans un pôle de compétence, parce que l'on ne pourra pas donner cette qualité à l'ensemble des acteurs judiciaires.
Rêvons même un instant que ce pôle puisse avoir les moyens suffisants pour être à la hauteur d'un défi extrêmement lourd parce que les lois votées en matière de cybercriminalité sont complexes et leur mise en œuvre est toujours coûteuse.

Le coût des expertises, et la pression du temps qui court , peuvent donner et inspirer le désir de ne pas approfondir. C'est d'ailleurs le deuxième facteur, celui de la loi. Il est excellent que les parlementaires puissent participer à nos échanges, parce que rien n'est moins évident que les deux difficultés auxquelles le juge est confronté en matière de cybercriminalité. La première, c'est ce que j'appellerai le syndrome du « *mille feuilles législatif* », l'empilement depuis trente ans de normes touffues et évolutives, l'appréhension trop complexe d'un corpus juris en matière de cyber-loi difficile à appréhender même par des spécialistes. Peut-être que certains dans la salle en sont capables mais pas au-delà. Deuxième chose, deuxième syndrome inquiétant, c'est la bonne vieille course entre gendarmes et voleurs. S'il y a un domaine où parfois l'on s'inquiète de voir le gendarme courir moins vite que le voleur, c'est bien le cybermonde puisque, par définition, les contraintes ne sont pas les mêmes et qu'elles sont vraiment beaucoup plus simples pour le criminel que pour le gendarme et l'acteur répressif. Nous avons donc besoin d'une rénovation et d'une simplification en tout cas d'une double remise en ordre. D'abord des textes, pour que les règles du jeu soient plus facilement accessibles, et ensuite, sans doute, du nombre quasiment illimité de structures publiques et privées qui ont mission à légitimement intervenir sur le champ de la cybercriminalité.

C'est vrai que celui qui aborde aujourd'hui la lutte contre la cybercriminalité aura de quoi avoir peur de se lancer, parce qu'il ne pourra pas en maîtriser facilement tous les contours. Il ne pourra compter ni sur une pause normative, ni sur un gel de la technologie. C'est dire la difficulté à rechercher et à trouver de la cohérence. C'est enfin sur un troisième facteur que j'aimerais bien insister : S'il y a bien une chose que l'on a appris avec la lutte contre la cybercriminalité, c'est qu'on ne lutte pas seul. En matière judiciaire, on ne peut jamais lutter seul mais ici c'est particulièrement le cas. On voit bien à quel point la coopération et la coordination sont l'alpha et l'oméga d'une lutte qui ambitionne de réussir. Le fait que vous ayez dans un court instant l'intervention des représentants d'Eurojust et d'Europol et un exemple d'un pays ami, vous démontrera à quel point ces dispositifs se développent et sont devenus consubstantiel à la lutte judiciaire contre la cybercriminalité.

On sait que les cybercriminels, qui sont des criminels tout court, ne se sont pas attardés pour découvrir les avantages du cybermonde. On voit à quel point l'internet peut être un outil redoutable dans les matières comme les atteintes aux intérêts personnels, à la dignité des personnes, aux intérêts financiers et aux intérêts des États.

La réponse passe toujours par les réseaux opérationnels. Le principe de confiance qui a été évoqué ce matin doit être explicitement mis en place dans les coopérations, nous en avons de bons exemples. La mise en place d'accords bi-latéraux peut rendre de moins en moins confortables les cyberparadis. Enfin, je crois qu'il faut ne jamais perdre de vue que le développement des armes numériques des cyberpatrouilles, des possibilités d'interventions à distance, doit toujours être proportionné à la défense de nos libertés. Ne noyons pas le bébé avec l'eau du bain, mais, à l'évidence, tout développement du cybertraitement de la criminalité par la justice doit s'accompagner de précautions.

Je voudrais pour conclure ces propos introductifs, vous suggérer de partager la réflexion d'un célèbre blogueur américain Evgeny Morozov. Je recommande et je n'ai pas d'intérêts dans

la maison, la lecture de son dernier ouvrage qui porte un joli titre en anglais « *The Net delusion* », et qui du côté français a été traduit par « *Le côté sombre d'internet* ». L'amateur de la guerre des étoiles que je suis s'en réjouit, car il nous faut conjuguer deux choses vraiment importantes pour nos réflexions aujourd'hui et demain. D'abord se méfier des cyberutopistes qui pensent que le net va générer tout seul les remèdes aux difficultés qu'il a contribué à créer ou à développer. Deuxièmement, se méfier tout autant des apôtres du « *tout internet* » qui estiment qu'un tel espace de liberté ne doit en aucun cas être contrôlé et surveillé par les institutions des pays. Je crois qu'une fois que l'on a compris ce dilemme, on peut avancer et espérer coopérer avec des outils efficaces.
Comme je suis magistrat et donc que j'aime les traditions, pour aller un peu plus loin que le XIXème siècle, je crois que l'on a depuis longtemps des éléments de réponse qu'il faut méditer toujours. Je terminerai en effet en citant un des pères de la stratégie militaire, le général Sun Tzu qui, il y a 25 siècles, nous avait montré le chemin à suivre, en indiquant que celui qui connaît l'autre et qui se connaît lui-même peut livrer sans bataille sans jamais être en péril. Voilà ce que je vous souhaite.

Général Jacques HEBRARD

Merci pour ce point de vue exprimé par la haute autorité que vous êtes. Une question est posée: aujourd'hui estimez-vous les magistrats suffisamment armés pour faire face à ce nouveau défi que constitue la cybersécurité et la cyberdélinquance ?

Yves CHARPENEL

Est-ce vraiment une question ? Non bien sûr... On voit bien que l'on découvre le fait que l'on ne peut plus se passer d'un réflexe et d'une compétence cybercriminalité. Aujourd'hui dans le monde opérationnel les enquêtes sont toujours d'autant plus complexes que celui qui doit diriger et qui doit poser les questions est parfaitement étranger à la matière de la cybercriminalité. Pour éviter des souffrances qui me paraissent bien inutiles et contre productives, je suggère de recourir énergiquement à la formation pluridisciplinaire. J'ai le privilège cette année de prendre la suite d'un magistrat compétent, un des rares en la matière, Myriam Quemener, pour diriger la session de formation continue des magistrats en matière de cybercriminalité. Il s'agit de reposer les bases car il y a un problème culturel qu'il faut franchir ensemble. A l'évidence, dans ce domaine aussi , notre marge de progression est importante.

Général Jacques HEBRARD

La parole est à monsieur Quillé qui pourra nous présenter l'activité d'Europol en matière de cybercriminalité puis nous dire certainement quelques mots sur le nouveau centre qui a été créé au début de ce mois.

Michel QUILLÉ

Je voudrais réagir en disant que je vais faire une présentation d'un caractère optimiste et mesuré eu égard à ce qu'a dit monsieur Charpenel. Il est vrai qu'il faut l'être lorsque l'on s'attaque au domaine de la cybercriminalité. Europol est l'agence européenne en charge de soutenir les enquêtes conduites dans les États membres en matière de criminalité organisée et de terrorisme. Notre siège est à La Haye. 27 États membres plus 10 États, associés par des accords de coopérations, sont représentés.

Au total, 800 fonctionnaires dont 150 officiers de liaison représentant de services opérationnels ou d'enquête tels que la police, la gendarmerie et les douanes pour la France. Ces chiffres incluent les membres de 7 agences américaines représentées à Europol, dont le FBI et la NCIS, ce qui témoigne de l'intérêt et de la crédibilité qui peuvent nous être accordé en toute modestie.
Europol soutient les enquêtes d'états membres en matière de criminalité organisée, incluant la cybercriminalité de la façon suivante : nous centralisons les renseignements qui nous sont communiqués par les états membres pour les agglomérer dans une base de données et dessiner les réseaux criminels, ce qui est un préalable à leur démantèlement. La question de la détection et du dessin de réseaux criminels concerne bien entendu la cybercriminalité. Pour rentrer dans le vif du sujet, Europol a été chargé par la Commission européenne, le 28 mars 2012, de créer le Centre européen de lutte contre la cybercriminalité. C'était la place naturelle de ce centre à Europol, parce que nous disposions de ce système de rassemblement de policiers et de réseaux. Le rôle de la France a été prééminent puisque c'est sous la présidence française de l'Union européenne en 2008 que l'idée a été lancée de créer à Europol l'embryon de ce centre, à l'époque le HTCC « *Hight Tech Crime Center* ». Vous voyez que la France avait déjà perçu le problème et lancé les pistes pour le régler.
Pourquoi une dimension européenne ? Comme cela a été souligné par monsieur Charpenel, la question de la cybercriminalité dépasse l'échelle européenne. C'est une problématique mondiale mais il faut préciser que l'Union européenne a un taux de pénétration de l'Internet de 67% contre 30% dans l'ensemble du monde, ce qui fait de nous une des cibles évidentes des cybercriminels.
La deuxième raison est que nous avions travaillé depuis plusieurs années sur ces phénomènes qui entrent dans le concept de cybercriminalité et nous avions des équipes d'enquêtes, des fichiers qui étaient spécialisés. Nous avons soutenu de nombreuses enquêtes, conduites dans les États membres et impliquant 13, 14, 15 États membres, avec des résultats certains qui ont permis de démanteler ces réseaux de pédopornographes. Dans un autre domaine nous travaillons depuis plusieurs années, sur la fraude aux cartes bancaires pour laquelle internet est un support évident et idéal. Récemment en décembre dernier, avec 13 États membres de l'Union européenne et 4 États hors Union européenne, nous avons aidé à démanteler un réseau de fraude aux cartes de crédit qui avait pris une dimension mondiale. L'atelier de confection des cartes utilisées par le biais d'internet était en Bulgarie. Les transferts se faisaient jusqu'au Pérou avec un retour dans l'Union européenne via la République Dominicaine. Vous constatez que la dimension mondiale est évidente.
La troisième raison de la création au niveau européen est que, dans l'Union européenne, le niveau de compétence ou de développement des instruments de lutte contre la cybercriminalité est très disparate. Certains d'états membres de l'Union européenne sont pratiquement au degré zéro, non par défaut de volonté mais du fait d'un problème de moyens. Europol aura un rôle à jouer dans ce contexte.
Le dernier point est que la position centrale d'Europol en terme de centralisation du renseignement en matière criminelle, donne une vision assez exhaustive de ce qui se passe. Cette position explique notre sollicitation par la Commission européenne quant à la confection d'un document que nous produisons depuis plusieurs années qui est « *l'état de la menace dans l'Union européenne* » que nous appelons

« *organised crime for assessment* ». La cybercriminalité faisait partie des priorités définies dans la dernière version de 2011. Nous sommes en train de préparer le SOCA, « *serious and organised crime assessment* ». Ses éléments font apparaître que le nombre des priorités sur lesquelles nous allons devoir enquêter dans l'Union européenne se réduit mais que la cybercriminalité reste l'une des priorités. Cela nous conduit à considérer que le cybercrime doit faire partie de nos travaux.

Comment cet European Cybercrime Center, que nous avons baptisé EC3, fonctionne-il ? Son mandat recouvre trois formes de criminalité dont l'Internet est le soubassement. La première concerne les délits commis par des groupes organisés, plus particulièrement ceux générant de larges profits tels que la fraude en ligne, ce que je décrivais avec la fraude aux cartes de crédits. Le deuxième domaine, qui n'est pas moins important à prendre en compte, est celui des dommages sérieux aux victimes de l'exploitation sexuelle des enfants. Le troisième des domaines touche les délits affectant les infrastructures et les systèmes d'information de l'Union. Ceci n'est pas notre priorité, puisque des institutions comme l'ENISA sont en charge de ce domaine mais nous pouvons y apporter notre expertise. Nous avons un mandat qui nous donne une certaine orientation et nous procurons un support opérationnel aux enquêtes. Nous avions trois grandes bases de données que nous avons fusionnées, l'une concernait la pédopornographie sur internet, l'autre les fraudes en général sur Internet et la troisième, tous les phénomènes de hacking bien connus et répertoriés.

Ce soutien aux enquêtes ne s'arrête pas là, parce que dans un domaine que nous défrichons tous ensemble, il y a la nécessité de développer ce que l'on appelle la police scientifique ou le forensic pour reprendre une terminologie anglo-saxonne. Ce forensic est partageable et nous sommes en train de créer ce que nous appelons un cyberlab. Ce soutien technique sera très important à partager car, dans ce domaine, certains États membres de l'Union européenne ont une faible capacité technique en matière de lutte contre la cybercriminalité alors que d'autres, je pense aux Pays-Bas, à la France et à la Grande-Bretagne, ont un système de lutte, sous l'aspect technique notamment, très développé. Nous n'allons pas réinventer la roue mais nous allons utiliser ce qui se fait de bien ailleurs. Nous avons un troisième domaine dans lequel nous voulons aussi investir à plus long terme, monsieur Charpenel le disait, qui est celui de partager les connaissances sur le principe de la confiance. Dans cette optique, nous avons dans l'idée ambitieuse de créer une cyberacadémie. Elle associera bien sur les universités, celles qui en tout cas investissent dans le domaine de la cybercriminalité. Ce système de cyberacadémie sera ouvert à tous les intervenants du domaine de la sécurité et de la justice parce que je crois que comme vous l'avez dit, il faut échanger, coopérer.

Quelles sont les perspectives pour conclure ? Dans les perspectives immédiates on retrouve la question de la coopération avec le secteur privé bien que les pouvoirs publics ne doivent pas perdre la main pour des questions de souveraineté, de possession des données. Néanmoins, je crois que dans ce domaine là, les services, ont une révolution culturelle à faire parce que les policiers et les gendarmes sont compétents mais cette compétence très technique ne s'invente pas. On ne pourra pas faire émerger un policier comme spécialiste de la criminalité, de la cybercriminalité en deux, trois ans alors que dans le secteur privé, il existe des spécialistes

qui sont à même de nous faire beaucoup avancer.
Cette coopération avec le secteur privé prendra deux formes. Une coopération déjà existante avec les grandes entreprises du secteur privé du domaine de l'internet, je pense à Microsoft, Google et d'autres qui sont partageuses. Nous pourrons bénéficier de leurs outils techniques qu'elles peuvent nous faire partager et ce que nous allons faire sera bénéfique pour elles également. Le deuxième volet de cette coopération avec le secteur privé sera le recrutement de personnels du secteur privé avec une compétence technique qui nous fera beaucoup avancer.
La coopération, la lutte contre la cybercriminalité ne peuvent être basées, vu la dimension du phénomène, que sur la coopération internationale policière et judiciaire, les deux étant bien entendu très imbriquées. Interpol va créer un centre qui couvrira le monde entier et qui va être inauguré en septembre 2014 à Singapour. Bien entendu, la coopération entre nous est commencée et elle sera obligatoire afin d'éviter notamment la duplication des moyens et le gaspillage des moyens financiers. Je voudrais terminer sur une note d'espoir, mais en mentionnant qu'il reste beaucoup à faire, mais je suis relativement optimiste.

Général Jacques HEBRARD

Merci pour ce point très complet sur Europol où vous mettez aussi en exergue le vrai problème de la formation. Mais nous pouvons déjà faire un constat de l'importance que va prendre la formation universitaire ou spécialisée dans le domaine de la cybercriminalité avec parfois une inquiétude. Depuis le début de ce forum on évoque la difficulté à trouver des ingénieurs. Je pense que le milieu universitaire, qu'il soit français ou européen, a effectivement besoin d'une véritable prise de conscience dans ce domaine afin de pouvoir anticiper un besoin qui va être croissant.

Michel QUILLÉ

Nous aurons l'obligation de nous aligner sur les salaires du secteur privé ce qui risque de poser problème. Nous demanderons pour cela un budget conséquent à la Commission européenne et je suis sûr que nous l'obtiendrons.

Général Jacques HEBRARD

Je propose que nous passions d'Europol à Eurojust et je vais donc demander à madame Sylvie Petit-Leclair de nous faire une présentation succincte de cet organisme qui, à mon avis, reste méconnu.

Sylvie PETIT-LECLAIR

Merci mon général. Je suppose que tout le monde avant d'arriver ici, connaissait Europol ; d'ailleurs ce matin, j'ai entendu citer au moins deux fois Europol mais jamais Eurojust, alors que notre rôle est bien complémentaire. En effet, généralement, si la police poursuit des malfaiteurs, ces derniers doivent tout de même être jugés. Il y a évidemment un juge qui intervient à la fin des investigations et des poursuites pour que les délinquants puissent effectivement être sanctionnés.
Eurojust est née d'une idée qui a émergé lors d'un Conseil qui s'est tenu en octobre 1999 à Tampere en Finlande. Il faut que vous sachiez que la coopération judiciaire est beaucoup plus récente que la coopération policière. Au cours des 50 dernières années, nous avons signé des conventions, divers textes qui étaient plus ou moins obligatoires, plus ou moins bien

appliqués mais en tout cas la coopération judiciaire n'était pas aussi aboutie que la coopération policière. Donc des chefs de gouvernement, des ministres ont, au cours de ce Conseil européen de 1999, estimé qu'il était important pour la coopération judiciaire qu'une agence spécialement dédiée à cette coopération judiciaire soit créée. C'est finalement au début de l'année 2002 qu'Eurojust a été officiellement inaugurée à La Haye, une agence provisoire s'étant brièvement installée à Bruxelles, mais finalement, pour des questions pratiques, il a été vite admis que nous devions nous trouver à proximité géographique, physique d'Europol.

Eurojust est en réalité une agence européenne, qui se trouve être à la disposition des magistrats pour favoriser la coopération judiciaire, pour la stimuler. Vous avez compris, et Monsieur Charpenel a mis l'accent sur ce point : la coopération, précisément dans le domaine de la cybercriminalité, est essentielle. C'est là la première mission d'Eurojust. Mais une autre mission qui n'est pas moins importante lui incombe : elle doit améliorer et stimuler la coordination des enquêtes et la coordination des poursuites entre les autorités compétentes des états membres.

Il nous est demandé de faciliter, en tout cas, de trouver des mesures adéquates pour stimuler cette coopération et favoriser la résolution d'affaires judiciaires. Eurojust peut également demander aux autorités compétentes des états membres concernés d'enquêter ou de poursuivre des actes spécifiques ou encore de coordonner des poursuites comme je l'ai dit. Eurojust peut également demander aux pays de s'entendre pour que l'un d'entre eux puisse être choisi comme étant celui qui est le mieux placé pour poursuivre des faits. Effectivement, dans le domaine de la cybercriminalité, ce point est extrêmement important puisque l'infraction commise peut être poursuivie dans plusieurs pays. Il est dès lors essentiel que l'un d'entre eux prenne le leadership ou en tout cas que les autorités judiciaires de l'un et de l'autre pays, ou l'un et les autres pays, puissent s'entendre pour que précisément il n'y ait pas de doubles poursuites. Dans le jargon judiciaire, nous disons qu'il existe un principe ne bis in idem, qui interdit de poursuivre et condamner surtout condamner une personne pour les mêmes faits. Par conséquent, Eurojust tente précisément de déterminer le pays qui sera compétent pour poursuivre et ce pour écarter, préventivement, le risque de voir ce principe ne pas s'appliquer.

Nous pouvons également favoriser la mise en œuvre d'équipes communes d'enquête. Monsieur Quillé en a parlé tout à l'heure, une équipe commune d'enquête est un moyen de coopération relativement abouti, puisqu'il permet à des magistrats de se transmettre des éléments de procédures, des éléments de preuves sans qu'ils soient obligés de faire des demandes d'entraide. Les policiers d'un pays vont travailler avec ceux d'un autre pays. Je considère à titre personnel que ce moyen doit être utilisé. Il m'apparaît effectivement important, on a parlé tout à l'heure de confiance, que des enquêteurs puissent travailler en pleine confiance avec des collègues, qu'ils puissent comprendre leur façon de travailler. Alors qu'autrefois on entendait systématiquement, assez souvent en tout cas, dans les services de police ou de gendarmerie, des critiques sur la façon de travailler de collègues étrangers, sans se préoccuper de savoir par exemple si le système juridique, l'arsenal juridique d'un autre état étaient différents et n'imposaient pas une méthode de travail différente. Donc l'équipe commune d'enquête m'apparaît être un moyen d'entraide et de coopération extrêmement abouti, non seulement en raison des avantages

qu'elle offre, c'est-à-dire encore une fois la possibilité de transmissions rapides d'informations croisées, mais encore en raison de l'ouverture qu'elle constitue pour les enquêteurs et les magistrats, qui comprennent, qu'à défaut de pouvoir être harmonisés, des systèmes différents coexistent.
Comment travaille Eurojust ? Les 27 pays de l'Union européenne sont bien sûr représentés à Eurojust. Il existe par pays un membre national, quelques fois un adjoint, quelques fois des assistants, comme pour le cas de la France. Au bureau français, il y a donc quatre magistrats et deux secrétaires qui, elles, font partie du personnel Eurojust. Nous travaillons également aux côtés de trois procureurs de liaison qui sont physiquement installés à La Haye dans les locaux d'Eurojust. Ils sont respectivement américain, norvégien et croate jusqu'à ce que la Croatie entre dans l'Union européenne, et nous travaillons quotidiennement avec eux comme avec les autres membres nationaux des Etats membres de l'Union européenne.
Nous avons aussi signé des accords de coopération avec d'autres agences : un accord de coopération bien sûr avec Europol, avec l'OLAF, avec un réseau de coopération d'Amérique Latine, ce qui est très intéressant évidemment pour les dossiers relatifs à la lutte contre les produits stupéfiants. Nous avons une liste assez importante de points de contact dans le monde entier, par exemple en Argentine, en Bosnie-Herzégovine, au Brésil, au Cap vert, au Canada, au Kazakhstan, au Liechtenstein, en Moldavie, en Mongolie, au Monténégro, etc.
Quel est le champ de compétence matérielle d'Eurojust ? en d'autres termes, de quelles infractions Eurojust peut-il être saisi ? Et bien, cette liste est très longue, très importante et se termine par une formule relativement générale qui permet en réalité d'englober le maximum d'infractions dès lors que plusieurs pays sont concernés. Sont concernés la criminalité organisée et le terrorisme, cela va de soi, mais aussi les infractions contre les enfants, le trafic d'être humains, les réseaux d'immigration clandestine, la corruption, le blanchiment, etc., et bien sûr la criminalité informatique. La formule générale dont je vous parlais précédemment est celle-ci : toutes autres formes de criminalité grave et transnationale.
Comment saisit-on Eurojust ? Ces propos s'adressent à mes collègues, aux policiers ou aux gendarmes, en tout cas, aux praticiens puisqu'il est apparu, pendant un certain temps, qu'Eurojust pouvait être une grosse machine administrative, que l'on ne pouvait pas saisir extrêmement facilement. En réalité c'est tout simple, un coup de téléphone ou un courriel suffisent. Nous disposons de messageries électroniques qui fonctionnent très bien et surtout d'outils qui nous permettent de communiquer depuis Lille par exemple.
Il faut que vous sachiez qu'Eurojust ne peut pas s'autosaisir Eurojust doit être saisi par un procureur ou par un juge d'instruction, en tout cas par une autorité judiciaire. On ne peut également être saisi que lorsqu'un dossier a été ouvert en France, lorsqu'il y a une enquête judiciaire. On ne pourrait pas dire par exemple que la cybercriminalité est très importante en France et qu'un dossier concernant cette forme de criminalité doit être ouvert. Il faudrait que le procureur de Paris, par exemple, me dise : « *J'ai une enquête préliminaire qui est diligentée actuellement en France, je parle d'ailleurs d'un dossier en particulier, et je souhaite qu'Eurojust intervienne puisqu'un certain nombre de pays, pour certains, membres de l'Union européenne et pour d'autres, pays tiers, sont impliqués. Je souhaiterais qu'une coordination des poursuites puisse être effectuée sous l'égide ou avec l'aide en tout cas d'Eurojust* ».

Dans un tel cas, lorsque nous recevons un dossier, nous l'examinons bien évidemment. Nous pouvons alors décider d'organiser une réunion avec les seuls membres nationaux d'Eurojust afin de voir à quel stade se trouvent les enquêtes respectivement diligentées par les autorités nationales de chaque pays, mais il nous arrive extrêmement fréquemment d'organiser, ce qui constitue le point d'orgue de notre travail, des réunions de coordination auxquelles participe l'ensemble des magistrats qui sont concernés par les faits considérés. Au cours de ces réunions de coordination, les autorités judiciaires des pays concernés décrivent les investigations en cours, exposent également leur besoin de coordination, leur besoin d'entraide judiciaire. Les autorités judiciaires des pays représentés peuvent évidemment décider d'émettre une commission rogatoire internationale, soit une demande d'entraide, ou encore suggérer la mise en place d'une équipe commune d'enquête. Ces réunions de coordination se déroulent le plus souvent, en présence d'Europol qui est pratiquement représenté dans chaque dossier, en tout cas, dans les dossiers les plus importants. Europol est invité à participer aux réunions de coordination qui sont organisées dans nos locaux, tout comme Europol nous invite lorsque des enquêteurs sont réunis autour d'une table dans les très beaux locaux d'Europol. Tout ceci pour vous montrer qu'il existe également une coopération, au niveau des deux institutions, un véritable travail en symbiose, ce qui me paraît évidemment important.

Au cours de ces réunions, il peut décidé, de mettre en place une équipe commune d'enquête mais aussi de fixer une date au cours de laquelle seront effectuées des opérations simultanées de police, dont des interpellations, des perquisitions et notamment bien entendu dans le domaine de la cybercriminalité. Il m'est arrivé, je n'étais pas encore à Eurojust mais au Parquet général de Paris, à la demande du Bureau français d'Eurojust, lui-même sollicité par les autorités espagnoles, de diligenter une enquête pour d'abord identifier et localiser les personnes qui avaient pu charger, télécharger et regarder des photos pornographiques d'enfants. Je crois me rappeler que 32 ou 35 Parquets français étaient concernés par cette affaire. Je me suis donc occupée de la coordination française. Les 35 procureurs de la République ont demandé aux enquêteurs de leur secteur de bien vouloir interpeller les personnes soupçonnées, à la même heure, le jour fixé lors de cette réunion de coordination organisée dans les locaux d'Eurojust, et d'accomplir des perquisitions et de saisir le matériel informatique.

Il s'agit là d'un véritable travail opérationnel. Je souhaitais en effet vous montrer qu'Eurojust n'est pas seulement une vitrine du Conseil, de la Commission en tout cas de l'Union européenne. Cette agence a été installée pour participer à la lutte contre le crime organisé. Je pense vous avoir démontré qu'elle est effectivement à la disposition de tous les praticiens et qu'elle accomplit un véritable travail opérationnel.

Il existe également au sein d'Eurojust des « *équipes* » qui travaillent de façon plus institutionnelle ; à cet égard, un « *team* », s'occupe de la délinquance économique et financière et un sous-groupe de ce groupe est précisément chargé de la cybercriminalité. Ce groupe milite pour favoriser la mise en œuvre d'équipes communes d'enquête mais également pour améliorer la formation initiale et continue des magistrats. Ce point a été évoqué par monsieur Charpenel et j'ai moi même le grand honneur de participer à ce genre de formation.

Alors que j'étais procureur adjoint à Versailles, je me suis trouvée en charge d'un dossier qui

concernait une grosse société. C'était sans doute le premier dossier avec lequel j'ai dû me battre tout d'abord, parce que la matière était nouvelle pour moi, et parce que j'ai dû, pour rebondir sur ce qu'a dit précédemment monsieur Quillé, travailler avec des entreprises privées. Je crois qu'effectivement, je le disais d'ailleurs ce matin à madame Souvira qui est commissaire de police à Paris, tant les policiers, les gendarmes que les magistrats doivent avoir une autre culture. Nous, magistrats, sommes habitués à travailler avec des enquêteurs. Il va falloir désormais que nous nous mettions à la page, afin que nous puissions entrevoir cette possibilité, voire cette nécessité, de travailler avec des entreprises privées. C'est effectivement tout nouveau pour nous puisque nous n'avions pas été formés à cela.
J'espère vous avoir démontré ce qu'Eurojust peut faire dans l'intérêt des magistrats saisis d'infractions transnationales, ce qu'il peut faire dans le domaine de la cybercriminalité puisque s'il existe une seule infraction transnationale c'est bien le cybercrime.

Général Jacques HEBRARD

Pouvez-vous illustrer les activités d'Eurojust avec quelques chiffres ?

Sylvie PETIT-LECLAIR

L'année dernière, du 1er janvier au 31 décembre 2012, 1 533 dossiers ont été ouverts à Eurojust dont 42 concernent la cybercriminalité. Je puis vous dire qu'en 2011, 1 411 dossiers avaient été ouverts et simplement 23 en cybercrime. Le bureau français a ouvert plusieurs dossiers, dont un dossier concernant le piratage du site du ministère de la Justice français mais qui impliquait d'autres pays dans lesquels d'ailleurs se trouvaient les auteurs des infractions.
La France a participé le 6 mars 2012 à d'importantes opérations d'interpellations à la demande de l'Italie dans une affaire de pédopornographie. Le bureau français a également été impliqué dans la coordination d'enquêtes dans une grosse affaire d'escroquerie à la taxe carbone, infraction qui devrait à terme relever de la compétence du parquet européen.

Général Jacques HEBRARD

Merci beaucoup pour cette intervention. Je laisserai le représentant du Conseil de l'Europe intervenir en dernier. Je propose que monsieur le substitut général de la République démocratique du Congo nous dresse un état des lieux de la cybercriminalité en Afrique et nous dise ce qu'il attend de la coopération internationale dans ce domaine.

Monsieur Dieudonné Tharcisse KANYAMA MBAYABU

Messieurs, mesdames, il est vrai que tout à l'heure quand je suivais les propos des intervenants, je me suis dis à un moment donné que je n'aurais que peu de chose à dire. En fait je réalise que les problèmes sont les mêmes et nous laissent la possibilité d'exprimer la façon dont nous les appréhendons en Afrique.
A ce niveau tout récemment, il y a eu un état des lieux de ce qui a été fait sur la cybercriminalité en Afrique. On a travaillé avec des pays qui avaient des législations en matière de cybercriminalité , notamment l'Afrique du Sud, le Cameroun, le Maroc et le Niger. Ces pays ont des lois cadres qui ont permis de résoudre plusieurs phénomènes de manière pratique. D'autres pays sont aujourd'hui sans législation spéciale par rapport à la cybercriminalité, c'est

le cas de mon pays. En fait, en tant que juriste, je ne peux pas dire que dans mon pays il y a un vide juridique. Il existe des lois traditionnelles, classiques qui permettent de résoudre le problème. Il serait toutefois plus indiqué d'avoir des lois spécifiques pour être plus efficace dans la répression de cette criminalité. Au Cameroun, en matière de cybercriminalité, on a prévu une disposition légale qui ouvre carrément une porte sur la coopération internationale. L'Afrique du Sud dans la section 90 de l'acte 25 de 2002, prend en compte la nature internationale de la cybercriminalité en prévoyant la compétence des autorités juridictionnelles dès lors qu'un lien existe avec l'Afrique du Sud. L'Afrique du Sud est signataire de l'accord d'assistance mutuelle et du réseau de chefs de police de l'Afrique de l'Est.

Ce sont des dispositions plus ou moins particulières qui existent dans des États et qui permettent à ce moment là de résoudre plus ou moins la question. De manière générale, il se pose un problème récurrent car en l'absence des lois spécifiques, l'exercice devient vraiment difficile pour le magistrat ou le juge. Il doit faire une gymnastique pour essayer de trouver dans la loi générale les dispositions qui peuvent donner lieu à une qualification. Prenons le cas par exemple de la visite de sites de films pédopornographiques. Le juge résout la question en visant simplement la disposition qui réprime les atteintes aux bonnes mœurs. On essaie de qualifier l'escroquerie pour la fraude en matière de cartes. On trouve ainsi une disposition légale pour réprimer, parce que l'on ne peut pas laisser un vide, laisser le délinquant œuvrer à souhait. Il se pose donc un problème majeur d'actualisation de textes pour s'adapter aux infractions qui viennent avec les nouvelles technologies notamment la cybercriminalité. Une étude a été menée tout récemment pour déterminer les niveaux de priorité. On a envisagé, suite à ces travaux, la rédaction d'un ouvrage sur la thématique prioritaire de la cybercriminalité en Afrique. On envisage également celle de guides d'information et de bonnes pratiques à destination de groupes cibles et enfin la rédaction d'un modèle de charte de conduite dans le cyberespace à destination par exemple des écoles, des lycéens etc. Il y a aussi un projet de convention africaine de lutte contre la cybercriminalité et pour la sécurité. C'est en chantier mais nous espérons que cela va vite évoluer.

Qu'attendons-nous en matière de perspectives d'avenir par rapport à ce forum ? Nous faisons pratiquement le plaidoyer, comme l'ont dit mes prédécesseurs, de la formation. C'est impérieux, aujourd'hui car il y a chez nous un problème de la connaissance très faible de l'informatique. En Afrique, c'est vraiment un problème qu'il faut prendre à cœur parce qu'il faudrait arriver à sécuriser l'espace et en même temps garantir les investisseurs qui peuvent venir. Si les investisseurs viennent dans un pays où la législation n'est pas très outillée pour réprimer cette forme de criminalité cela pose un problème. La formation doit impérativement intervenir comme premier moyen pour lutter contre cette faiblesse. Nous pensons qu'il faut organiser la formation des formateurs pour qu'à leur tour ils puissent répercuter la même formation à d'autres personnes qui sont dans la chaîne pénale de répression. Nous pensons également qu'au delà de la formation, il faudrait également penser au renforcement des textes, des outils qui peuvent servir de base à la répression, parce que, si ces outils sont inexistants, ça sera difficile d'œuvrer avec une certaine sérénité dans le domaine. Enfin, nous pensons que le projet de convention africaine est important pour nous dans la mesure où, aujourd'hui, nous nous inspirons de ce qui existe en Europe. Il serait souhaitable d'élargir

les conventions européennes afin que l'Afrique puisse bénéficier des mêmes avantages pour lutter ensemble contre un phénomène transfrontalier.

Général Jacques HEBRARD

Merci monsieur le substitut général de cet état des lieux et puis aussi de cette analyse au niveau du continent africain, des problèmes liés à la cybercriminalité. C'est aussi le rôle de ce forum de permettre de fournir les outils ou de vous mettre en contact avec les spécialistes de la matière, en espérant que les représentants de cette coopération internationale pourront vous appuyer sur cette démarche nécessaire pour votre pays et votre continent.
Merci de cette intervention, nous allons conclure le panel avec monsieur Alexander Seger qui va nous faire un point au niveau du Conseil de l'Europe.

Alexander SEGER

Merci. Après une perspective française, une perspective de l'Union européenne, une perspective africaine voilà notre expérience avec le reste du monde. Je suis responsable au Conseil de l'Europe de la question cybercriminalité c'est-à-dire la Convention de Budapest qui n'est pas limitée à l'Europe d'ailleurs. Le comité sur la cybercriminalité, c'est le comité qui comprend les parties à la Convention et aussi les programmes de coopération et d'assistance technique. J'ai cinq propos et un souci. Le premier propos concerne, c'est un besoin très important, l'harmonisation de la législation au niveau global. Sans un cadre légal pas d'investigation et sans un minimum d'harmonisation pas de coopération efficace internationale.

La convention de Budapest sur la cybercriminalité offre un cadre pour la législation que n'importe quel pays dans le monde pourrait suivre. Nous avons récemment analysé les 193 pays membres des Nations unies, et nous avons constaté qu'au moins 140 pays sont en train de réformer leur législation ou ont déjà réformé leur législation sur la cybercriminalité. Les deux « *Congo* » ne font pas partie de ces 140 pays. Au moins 125 pays ont utilisé la Convention de Budapest comme ligne directrice ou au moins comme une source d'inspiration. Cependant beaucoup de pays ont besoin d'aide pour mettre entièrement en ligne ce traité. On a vu que beaucoup de pays ont pris une partie de la Convention mais le reste l'a mal comprise ou mal mise en œuvre. Il y a en fait une dizaine de pays africains qui ont des lois extraordinaires, le Sénégal, l'île Maurice, Botswana, l'Afrique du Sud et le Cameroun. Le Maroc est en train de réformer. Le meilleur projet de loi est au Niger depuis 2006. Il n'a jamais été adopté mais c'est un projet de loi extraordinaire.
Le deuxième propos, c'est utiliser la Convention de Budapest comme un cadre de coopération internationale. Pour nous c'est d'abord une question de quantité ; il faut accroître le nombre de parties à la convention et on a fait un bon progrès en 2012, quand l'Australie et le Japon sont devenus partie de la convention. On a maintenant 57 États qui ont soit ratifié, soit signé, soit étaient invités à la convention de Budapest. Le Sénégal a déjà été invité et quelques pays africains vont l'être. L'Afrique du Sud est signataire de la convention de Budapest. Mais c'est aussi une question de qualité. Il faut améliorer l'efficacité du traité et on a, en 2012, effectué une première série d'évaluations sur la mise en œuvre de la convention par les parties. Le rapport d'évaluation a été mis en ligne la semaine dernière. Nous avons analysé

comment les parties de la convention ont mis en œuvre les articles 16, 17, 29 et 30 sur la conservation rapide des données. En 2013 l'accent de l'évaluation sera porté sur l'efficacité de la coopération internationale. En décembre, j'espère que l'on va avoir aussi une évaluation de l'efficacité de la coopération internationale par les parties à la convention. Je crois que nous sommes en bonne voie avec la convention de Budapest.

Troisième propos, il y a un besoin d'accès transfrontalier par les investigateurs aux données stockées quelque part dans le nuage. Je crois qu'il y a déjà quelques intervenants qui ont déjà évoqué le problème des compétences territoriales dans un contexte de cloud computing. Les données en fait ne se trouvent plus sur les ordinateurs individuels, elles se trouvent quelque part dans les nuages souvent à l'étranger, souvent dans des localisations inconnues. Alors à qui demander une entraide judiciaire ? La convention de Budapest sous l'article 32, prévoit des possibilités très limitées d'accès transfrontalier mais on a aussi constaté que beaucoup de pays, beaucoup d'états aussi qui font partis de la convention de Budapest vont au-delà de l'article 32. Il faut alors clarifier ce que veut dire l'article 32 et il faut un cadre légal international plus clair pour les situations au-delà de l'article 32. Le comité des parties à la convention de Budapest a analysé cette question en détail en 2012 et en décembre a adopté dans son rapport une autre orientation pour faciliter une meilleure compréhension de l'article 32 mais aussi élaboré un protocole additionnel à la convention de Budapest. Cela montre aussi qu'il est bien possible d'ajouter des outils supplémentaires à la Convention de Budapest.

Quatrième propos, il faut des garanties, des sauvegardes pour limiter les pouvoirs de force de l'ordre et pour la protection des données. La liberté que nous offre internet est très chère à nous tous, il faut la protéger. Il est absolument nécessaire de respecter les droits de l'homme et nous insistons beaucoup sur l'article 15 de la convention de Budapest et aussi sur la cconvention 108 sur la protection des données personnelles dans notre coopération avec le pays tiers.

Cinquième propos, l'assistance technique est une exigence principale sur le niveau mondial pour renforcer les capacités de la justice pénale, la coopération à tous les niveaux. Les états doivent être en mesure d'appliquer leur loi. Et c'est pour ça que la question de formation évoquée par tout le monde n'est pas seulement un consensus banal, c'est un consensus international. Aux Nations Unies, tout le monde est d'accord sur l'assistance technique. Là on a pour une fois un consensus total mondial, c'est extraordinaire.

Pour autant, Il y a souvent des discussions internationales sur un nouveau traité international sur la cybercriminalité. A notre avis, ces discussions comportent des risques et vont certainement continuer dans quelques semaines à Vienne dans le groupe d'experts de cybercriminalité. depuis 10 ans Ces discussions confirment clairement qu'il n' y a aucun consensus international à commencer les travaux sur un nouveau traité. Mais, pour des raisons politiques, je crois qu'elles vont continuer. J'ai constaté la même chose il y a 2 ou 3 ans ici sur la même chaise : je crois qu`il y a trop d'enjeux politiques en la matière. Je crois que l'on a un consensus total entre les juges, entre les procureurs, entre la police de presque tous les pays mais il y a quand même des jeux politiques qui n'ont rien à faire avec la lutte contre la cybercriminalité. Nous voyons le risque que ces débats mettent l'accent sur le contrôle de l'internet par les gouvernements. Nous voyons que ces discussions

perturbent des réformes déjà en cours. Le Congo ne va jamais utiliser la convention de Budapest pour élaborer un projet de loi. Si vous attendez encore une convention des Nations Unies, cela va prendre peut-être 10, 15, 20 ans pour avoir un autre traité en place. On a vu que ces discussions mènent à une rupture des réformes dans beaucoup de pays. Et surtout, on l'a vu à Dubaï en décembre dernier, pendant le World Conference on international Telecommunications, il y a un risque que ce débat serve la division internationale. Il y a un risque d'une guerre froide dans le cyberespace comme l'ont montré les débats à Dubaï.

Général Jacques HEBRARD

Merci monsieur SEGER. Il me reste à remercier l'ensemble des intervenants pour les précieux éclairages qu'ils nous ont apportés dans le domaine de la coopération internationale européenne et dans le volet judiciaire en particulier.

LES CENTRES DE DONNEES DANS LE MONDE : 3 000 000
DOMMAGES MOYENS PAR CYBER ATTAQUE : 2 500 000 €
UN PARTENAIRE POUR LES SOLUTIONS DE SECURITE

SOLUTION DE CYBER SÉCURITÉ AVANCÉE. De nos jours, les gouvernements, les institutions, les entreprises et les autorités publiques échangent leurs informations grâce à des infrastructures IT et des réseaux de communication. Parallèlement, le nombre de cyber attaques sophistiquées augmente endommageant les données sensibles des systèmes d'information. Nous sommes fiers que les opérateurs du monde entier nous aient choisis pour nos excellentes compétences en matière de cyber sécurité. **www.cassidiancybersecurity.com**

CASSIDIAN
CYBERSECURITY

AN **EADS** COMPANY

EFFACEZ VOS SMARTPHONES ET TABLETTES AVEC CERTITUDE

ANDROID BlackBerry symbian OS iOS Windows Mobile

Pourquoi effacer les Smartphones ?

- Effacement définitif des données utilisateurs tels que emails, contacts, SMS, photos.
- Réutilisation du mobile en toute sécurité.

Pourquoi utiliser Blancco ?

- Effacement 100% sécurisé
- Processus rapide de traitement
- Le logiciel d'effacement de données le plus certifié du marché

blancco

CERTIFIED DATA ERASURE

Blancco - France S.A.S.
29/31 Rue du Chemin de Fer
59100 Roubaix, FRANCE

francesales@blancco.com
Tel. +33 (0)3.20.27.19.32

A1 - Géopolitique du cyberespace

Intervenants :

- Francois-Bernard Huygue : Chercheur à l'IRIS,
- Bertrand de la Chapelle : Membre du conseil d'administration de l'ICANN, directeur du projet « Internet et juridictions » à l'Académie diplomatique Internationale,
- Frederick Douzet : Maître de Conférence, Institut Français de Géopolitique, Université Paris 8,
- Jean-Jacques Lavenue : Directeur, IREENAT, Université de Lille 2,
- Kave Salamatian : Professeur, Université de Savoie,
- Daniel Shaeffer : Général (2S), consultant.

Résumé des interventions :

La relation entre cyberespace et géopolitique reprend des fondamentaux de cette dernière mais doit prendre en compte des données nouvelles. Enjeu de pouvoirs, le cyberespace est un autre territoire suscitant de nouveaux enjeux et la nécessité de trouver de nouvelles règles.

I. Les problématiques

D'emblée un paradoxe : comment la géopolitique, discipline déjà ancienne, peut nous aider à comprendre le cyberespace ?

La géopolitique est une discipline qui considère l'État comme un organisme géographique ou comme une entité dans l'espace. Avec le cyberespace, trois données sont à prendre en compte : l'existence d'une solide couche matérielle (tuyaux, câbles…), des conflits du monde réel reproductibles dans le monde virtuel et enfin l'installation d'un technopouvoir dans le cyberespace. Comment donc comprendre les rapports entre géopolitique et cyberespace ? Comment comparer ce système incertain de souveraineté technique au monde « westphalien » que nous connaissons?

La Chine est l'exemple même d'un grand pays qui a pris toute la mesure de la modernité et a su s'adapter en contrôlant ce qui était considéré comme incontrôlable, allant jusqu'à créer un Google et un Twitter chinois. Un questionnement existe quant à l'utilisation du cyberespace par la Chine sachant qu'il faut garder en mémoire une volonté très culturellement ancrée d'ambition et de domination du monde.

On peut également s'interroger sur les apports de la métrologie et de la cartographie des réseaux dans la compréhension du cyberespace sachant qu'Internet est, de manière incontestable, un nouveau territoire.

Un consensus général est retenu pour dire que la définition d'une norme juridique et la question du Web sont un enjeu politique dans le cyberespace.

II. Des solutions

Le cyberespace est un nouveau type de territoire qui n'entre pas dans la définition géographique classique sachant qu'il n'existe pas de définition consensuelle et objective du cyberespace.

La représentation du cyberespace comme territoire est une idée forte, partagée par les différents acteurs, mais qui n'en n'ont pas la même définition. Le cyberespace est un enjeu mais aussi un espace pour les rivalités de pouvoir où la notion d'autorité est très présente avec des acteurs ayant des formes nouvelles par rapport aux formes classiques. Ce ne sont pas uniquement les États mais aussi des acteurs comme les hackers, les pirates… L'élaboration d'une réflexion stratégique par rapport au cyberespace nécessite également une compréhension des enjeux géopolitiques, des rapports de force, des stratégies de contrôle et de pouvoir à la fois dans le cyberespace et en dehors de celui-ci.

Le terme cyberespace, très en vogue dans les années 90 et assimilé à un espace échappant à toute réglementation, avait disparu pour réapparaître pour des raisons inverses notamment d'enjeux de sécurité. Ce sont deux visions de représentation aussi dangereuses l'une que l'autre. En matière d'Internet et d'espace numérique, les frontières ne sont pas claires notamment parce que l'action d'une autorité publique sur un opérateur basé sur un territoire a potentiellement un impact sur les acteurs et les utilisateurs d'autres territoires. La géographie du cyberespace n'est pas euclidienne. Dans le monde de l'Internet, le fantasme de la réintroduction de la souveraineté limitée par des frontières clairement délimitées est une illusion dangereuse, le véritable enjeu étant la gestion des « *commons* ». Quant aux ordres juridiques qui se chevauchent, les défis auxquels nous sommes soumis consistent à trouver les instruments nouveaux qui ne soient pas seulement dédiés à une gestion commune de ces espaces.

Avec le cyberespace, la Chine en a pris la mesure des avantages (propagande intérieure et économie) et des inconvénients (vecteur de l'opposition et cybercriminalité). Les menaces chinoises visent avant tout l'économie avec les acquisitions légales et illégales. Elles s'inscrivent également dans le cadre de la confrontation sino-américaine où la Chine voit dans les USA une menace potentielle. Elle mène une guerre asymétrique en se dotant d'une véritable muraille cybernétique.

La cybergéographie est peu connue car pluridisciplinaire. A titre d'exemple, l'Inde et la France sont géographiquement lointaines mais aussi directement voisines par les routeurs. A quelques centimètres de distance on passe d'une juridiction française à une indienne. Nous sommes d'ailleurs, en cela, très proches des Américains qui sont des voisins curieux de tout le monde (gmail).

Historiquement les Américains sont les premiers à avoir « *monté* » un système avec l'ICAAN (Internet Corporation for Assigned Names ans Numbers). Ils sont dans une alliance objective avec les géants du WEB ce qui peut expliquer que certains États supportent mal cette hégémonie et souhaitent créer leur propre réseaux web comme le réseau « *Halal* ». Pour régler les conflits de pouvoir, la solution pourrait être l'UIT ou une sorte de SDN (Société Du Net), mais il est gênant que le débat soit réduit à deux thèses : soit le système américain avec l'ICAAN soit l'UIT (Organisation Internationale des Communications).

A2 - Souveraineté et Cloud computing

Intervenants :

- Daniel Guinier : Expert près la cour pénale internationale de la Haye,
- Bernard Carrayon : Avocat au barreau de Paris, ancien député,
- Luis Delabarre : Architecte sécurité – Thalès,
- Pierre Siaut : Cybersécurité – Trend Micro,
- Philippe Duluc : Directeur de la sécurité – Bull,
- Jean-Nicolas Piotrowski, président directeur général d'Itrust.

Résumé des interventions :

L'émergence de la technologie du Cloud modifie la relation entre le client et le founisseurr. Les conditions juridiques de détention et de gestion de la donnée conditionnent une gouvernance et une sécurisation des transactions. Elles impliquent de fait une souveraineté territoriale. La France comble un droit lacunaire par des dispositions textuelles préservant la propriété intellectuelle, le secret des affaires et la protection de domaines sensibles.
La sécurisation des transactions passe par l'application de protocoles reposant sur la fragmentation des données, des techniques de chiffrement, des couches de virtualisation sécurisées et l'application de normes émergentes. La dimension contractuelle entre le CSP et le client doit comporter le régime de la donnée et une fonction d'audit externe propre à la distinction entre la sécurité et le contrôle.

Le développement du « *Cloud* » provoque une rupture dans la relation client-fournisseur et le fonctionnement de l'entreprise. Il s'agit d'une triple révolution en terme économique, de sécurité et de souveraineté. Une forte demande économique repose sur la « *virtualisation* » permettant de modéliser, paramétrer, et d'exploiter une ressource informatique indépendamment des matériels, de consacrer l'émergence d'une culture de business modèles par la location d'applications par Internet et une variabilisation du stockage de la donnée sans dépenses d'infrastructure. Cela permet de consacrer la ressource financière au R&D, ce qui intéresse les start-up qui peuvent tester leurs services sans autres frais.

I. Un enjeu de souveraineté et de sécurité

L'enjeu est celui de la sécurisation technique et juridique et de la confiance entre client et opérateur. Le recours aux clouds américains a des conséquences négatives sur la sécurité, la confidentialité des données et la vie privée des citoyens européens. Le Patriot Act permet

la consultation d'informations liées à la vie privée dans les entreprises et les organismes. L'Europe est fragilisée sur une problématique de compétence territoriale. La France relève cet enjeu de souveraineté.
La législation française relative à la loi sur le secret des affaires concerne les informations protégées quel que soit leur support. Le décret n° 2011-1425 du 2 novembre 2011 relatif à la protection du potentiel scientifique et technique de la nation, institue des ZRR (Zones à Régime Restrictif) inhérentes aux intérêts de la nation. L'arrêté du 3 juillet 2012 vise les niveaux de protection lors de contrats d'externalisation des données et de prestations de service.
Les dispositions européennes envisagées pour 2013 concernent le concept d'une certification européenne, une normalisation et une compétitivité sans référence à une souveraineté européenne.
On doit également relever que le régime juridique de la détention et de la gestion de la donnée est régi par des considérations juridiques différentes selon le droit du pays où elle est stockée. A titre d'exemple, une approche différente intéressant le nazisme, les sectes ou les mœurs sexuels affectera différemment l'utilisateur et le détenteur de la donnée. On peut également s'interroger sur la disponibilité des données traitées par une voie judiciaire locale.
Le changement de fournisseur implique un contrat mutualisé différent qui prenne en compte spécifiquement l'effacement des données et leur désengagement du site. Une capacité d'audit par le client doit être préservée afin de déterminer une analyse du risque. On peut citer l'exemple d'un offreur dont une faille permettrait l'utilisation de données par un tiers impliqué dans une pratique pédopornographique. Le propriétaire de la donnée sera inclus dans la procédure. L'attaque de sites Playstation network de Sony, l'affaire Microsoft contre Botnet/Zeus ou Amazon/cloud comporte une analyse juridique qui cherche à déterminer le niveau de complicité de l'hébergeur.

II. Un arsenal technique émergent

Sur un angle technique, les données doivent être sécurisées au niveau des CSP1 par un chiffrement (algorythme, langage) et une gestion essentielle des clés. L'interopérabilité implique une possible perte de gouvernance et une gestion des clés en relation avec les standards émergents (CAMIP)2. Le cloud pose une difficulté quant à l'application au client de procédés de chiffrement notamment pour les PMI et PME qui n'ont pas cette capacité. La plupart ne disposent pas de plan de reprise d'activités (PRA). Il faut en conséquence privilégier des solutions fonctionnelles en relation avec la capacité de l'entreprise. L'usage va vers une IAS (Internet Authentification Service)3 qui procure une sauvegarde et une synchronisation des données et une gestion transparente des incidents entre le client et le CSP. Il ouvre à l'authentification des utilisateurs et des autorisations. Ces techniques impliquent une remise en question des acquis car la capacité de provisionning en mode automatique implique un chiffrement sur des logiciels et matériels adaptés malgré un parc hétérogène. Bien qu'insuffisante, la défense périmétrique des CSP (protection des clés) doit être une préoccupation des SSI.
Des pistes passent par l'usage de framework sécurisés, outils de contrôle et de répartitions des données dans le cloud. Il est recommandé

une fragmentation des données au sein du data center pour empêcher leur extraction. La traçabilité des preuves implique une supervision en temps réel qui, par une « *Virtual machine* », puisse scruter les « plugin » et effectuer un « *check* » permanent des mouvements vers le cloud provider. Un filtrage en sortie de cloud, notamment pendant les mises à jour, ainsi que l'inclusion d'une analyse comportementale, font partie des solutions. Une séparation des processus et DVM, modules inspectant les fichiers transitant selon des règles et signatures propres à leur format spécifique, constitue une gène pour les attaquants. L'analyse protocolaire à états par « *PVM et DVM* »[4] permet une protection accrue contres les attaques inconnues (zero-day). En matière de supervision du cloud et des systèmes de sécurité, la norme ISO 15408 est une référence qui peut constituer un élément de confiance. Il est nécessaire de mettre en place une supervision et un audit du check-act indépendant. Cette dualité répond à un besoin de sécurité réactive selon l'évolution de la menace et d'obtenir un réel examen du système par une différenciation des fonctions de sécurité et de contrôle .

La solution cloud français, paramétré pour éviter les déports sur des clouds externes pour des problèmes de taille critique, avec application d'un droit local, assurerait la sécurité des informations. Cela procurerait un avantage aux administrations et aux entreprises.

Le Cloud communautaire peut-être une solution pour des clients publics et privés. On peut également envisager la solution d'un cloud privatif. Il subsiste la question de la gestion des clés, mais une des conditions essentielle, réside dans le fait que les entreprises doivent utiliser des systèmes proches afin de permettre une satisfaction suffisante du client.

1 - Le principe du trading haute fréquence : acheter au moins cher et vendre au plus offrant toutes les microsecondes pour dégager une faible marge de très nombreuses fois.

A3 - Clusif - Panorama de la cybercriminalité, année 2012

Intervenants :

- François Paget : Secrétaire Général du CLUSIF, chercheur chez McAfee Labs.

Résumé des interventions :

En 2002, le CLUSIF présentait son premier Panorama de la Cybercriminalité. Depuis onze ans, cet exercice éclaire le public sur les tendances du moment et l'émergence de nouveaux risques. Il permet de relativiser et de mettre en perspective des incidents qui ont, à tort ou à raison, défrayé la chronique. A partir de 2009, le panorama s'est élargi aux événements accidentels et aux faits de société pouvant induire ou aggraver des actions cybercriminelles. La sélection des sujets est réalisée par un groupe de travail pluriel constitué d'experts en sécurité venant du privé comme de l'administration. Les informations utilisées proviennent exclusivement de sources ouvertes.
L'édition 2013 du Panorama, présentée au FIC, s'est focalisée sur cinq grands sujets.

I. Ni la fin du monde, ni la fin des accidents…

Même si les événements accidentels ne sont pas stricto-sensu de la cybercriminalité, les pannes et les accidents font partie des risques numériques. Et 2012 n'a pas échappé à son lot d'incidents (Blackout électrique en Inde, panne chez Orange, tempête aux USA). En août, Knight Capital, un poids lourd de Wall Street, spécialisé dans le trading haute fréquence [1], frôle la banqueroute suite à un bug informatique. Les pertes sont estimées à 440 millions de dollars. Par quatre fois, en 2012, le cloud Amazon fait face à des incidents très classiques (bugs, pannes électriques, etc.). Une réaction en chaine entraine nombre de ses clients dans la tourmente. Pour le CLUSIF, ces événements sont aussi une source potentielle d'inspiration pour les cybercriminels qui cherchent à étoffer leur palette d'attaques et identifier de nouvelles failles.

1 - Le principe du trading haute fréquence : acheter au moins cher et vendre au plus offrant toutes les microsecondes pour dégager une faible marge de très nombreuses fois.

II. Cyber-conflits et attaques ciblées

2012 a été marquée par de nombreuses prises de positions officielles au sujet de la gestion des cyber-conflits. Pour le CLUSIF, la militarisation du cyberespace est enclenchée. Elle passe par un renforcement des capacités défensives, voire offensives, des États qui recrutent des spécialistes, publient des

documents stratégiques, affinent leur communication et mènent des cyber-exercices. Même si, en 2012, aucune cyberattaque n'a été revendiquée ou clairement attribuée à un État, l'approche décomplexée de certains d'entre eux en la matière, promet, selon le CLUSIF, d'importants bouleversements.
Autre constat du CLUSIF : les attaques informatiques ciblées se sont amplifiées en 2012 tant par leur nombre que par la richesse de leurs modes opératoires ou par leur gravité (malware Sykipot et Mirage, piratage de la NASA, de l'agence spatiale japonaise, de Verisign, du MoD britannique, etc.). L'implication des états à des fins d'espionnage a souvent été invoquée après ces découvertes mais les commanditaires n'ont jamais été à ce jour clairement identifiés. Le CLUSIF note cependant une corrélation entre ces attaques et des tensions préexistantes (géopolitiques, économiques, militaires, sociétales…) entre les protagonistes supposés. Il regrette aussi la tentation du sensationnalisme dans le traitement médiatique, contraire à la sensibilisation et préjudiciable au secteur de la sécurité. Toujours selon le CLUSIF, l'exagération et parfois même la désinformation sont susceptibles de brouiller, voire de décrédibiliser, le message sur les risques liés aux menaces informatiques.

III. Hack As A Service

Pour le CLUSIF, le commerce de la malveillance se porte bien. S'éloignant des forums underground, la nouvelle recette des pirates passe par la mise en place de sites de vente en ligne qui ressemblent à ceux de l'e-commerce habituel dans lesquels on achète et on paye en un clic, sans jamais se rapprocher du vendeur qui peut ainsi rester dans l'ombre. Pour améliorer la visibilité de ces sites, un marketing ciblé voit le jour. Les personnes susceptibles d'être intéressées par ce type de commerce reçoivent des courriels publicitaires annonçant de nouveaux produits ou des remises exceptionnelles.
L'apparition d'un « *grey market* » est aussi un phénomène émergeant. Le CLUSIF s'inquiète de voir apparaitre d'étranges sociétés de sécurité proposant des logiciels et des services pour lesquels on a parfois du mal à cerner les acheteurs potentiels. Sous couvert de s'adresser aux gouvernements et à leurs officines, ne sommes-nous pas en droit de nous interroger sur le fait qu'elles pourraient se laisser tenter par d'autres négociations auprès d'acheteurs moins honnêtes ? Ne dit-on pas que l'argent n'a pas d'odeur ?

IV. Les Botnets à toutes les sauces

En 2012, des études ont montré que les usages des botnets se sont multipliés. Précédemment utilisés pour l'envoi de spam, le DDoS et la collecte de données bancaires, des botnets d'un nouveau genre ont vu le jour pour de nouvelles formes de délinquance numérique à petite ou grande échelle. Ils s'adaptent ainsi aux nouveaux écosystèmes criminels qui se mettent en place. Le cas de Sality qui, en 12 jours (c'était en 2011) est arrivé à scanner plus de 86% des adresses IPV4[2] existantes, à la recherche de composants PABX IP (serveurs SIP) [3] vulnérables en est un exemple.

2 - Une adresse IP (avec IP pour Internet Protocol) est un numéro d'identification qui est attribué de façon permanente ou provisoire à tout appareil connecté à un réseau informatique utilisant l'Internet Protocol. IPv4 est la première version d'Internet Protocol (IP) à avoir été largement déployée. Elle forme encore en 2012 la base de la majorité des communications sur Internet, avec l'IPv6.
3 - SIP signifie Session Initiation Protocol. C'est un protocole de téléphonie utilisé pour établir, modifier et arrêter des appels téléphoniques VoIP. Un serveur SIP est le principal composant d'un PABX IP et gère tous les appels SIP du réseau (source FAQ watsoft).

V. Mobilité

Pour le CLUSIF, l'année 2012 aura été marquée par une spectaculaire envolée des malware bancaires sur mobiles. Après des mois de prospection, les cybercriminels semblent avoir trouvé le filon et se ruent à présent sur les données personnelles et financières des utilisateurs de Smartphone. Le développement exponentiel du marché de la téléphonie mobile, allié aux nouvelles vulnérabilités induites par le paiement sans contact, ouvre un nouveau territoire de chasse qui n'a rien à envier à l'Internet d'il y a 10 ans.
Il est aujourd'hui possible de prendre le contrôle d'un Windows Phone, d'un Android, d'un Symbian ou d'un iOS. Un attaquant peut secrètement écouter les conversations, localiser un appareil, installer une application via un lien compromis, prendre des photos ou encore placer des ordres d'achat sans le consentement de l'utilisateur. Selon le CLUSIF, le placement d'ordres d'achats concurrencera bientôt l'appel de numéros surtaxés.

Conclusion

L'année 2012 a donc été copieuse en événements. Pour François Paget, Secrétaire Général du CLUSIF et animateur de l'atelier 3 du FIC, d'un côté, « *les particuliers se retrouvent face à un nombre croissant de menaces sur les mobiles. Ces équipements, encore aujourd'hui peu protégés, vont devoir être considérés différemment par leurs propriétaires* » insiste-t-il. De l'autre, ajoute-t-il, « *les entreprises voient apparaître de nouveaux protagonistes aux côtés des cybercriminels et des hacktivistes. A la fin 2012, les États ne sont plus seulement vus comme protecteurs, spectateurs ou victimes, mais aussi, et c'est nouveau, comme concepteurs de cyber-armes.* »

A4 - Cyberdélinquance ou cybercriminalité organisée : Quels sont les profils des cybercriminels ?

Intervenants :

- Bruno Chapuis : Colonel, chargé de mission au STSI[2][1], Gendarmerie nationale,
- Éric Freyssinet : Lieutenant-colonel, chef de la division de lutte contre la cybercriminalité, Gendarmerie nationale,
- Valérie Maldonado : Commissaire divisionnaire, Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), Ministère de l'Intérieur,
- Boris Sharov : Président-Directeur Général, Doctor WEB.

1 - STSI² : Service des technologies et des systèmes d'information de la sécurité intérieure

Résumé des interventions :

L'analyse des actes de criminalité « *classique* » montre une corrélation entre crime et criminel. Ce système de corrélation est dépassé dans le contexte d'un cyberespace.
Il existe une réelle nécessité d'appréhender les profils des cybercriminels, de l'amateur au professionnel, de l'étudiant à l'organisation internationale. Cela constitue un enjeu majeur qui se révèle complexe, tant les profils sont multiples et encore trop rarement étudiés. Les cybercriminels s'affranchissant des frontières, ce travail d'identification doit s'inscrire dans un effort commun de coopération et d'échanges.L'édition 2013 du Panorama, présentée au FIC, s'est focalisée sur cinq grands sujets.

Historiquement les premiers actes de cybercriminalité étaient le fait de particuliers véhiculant l'image caricaturale d'un étudiant ou d'un passionné d'informatique. Sans entrer dans les clichés, ce profil était pourtant dominant chez les cyberdélinquants aux prémisses d'Internet. De nos jours, en revanche, les actes de cyberdélinquance se sont étendus. Délinquants et criminels, toujours dans une « habile politique d'innovation », ont entrepris d'exploiter au maximum ce nouvel espace, encore en construction il y a quelques décennies. Ainsi, aujourd'hui, les actes de cyberdélinquance et de cybercriminalité sont l'œuvre de personnes aux profils variés, balayant tout un spectre de professions, de personnalités et de moyens. L'essor de la cybercriminalité, les sommes et les informations mises en jeu sur Internet, en font désormais une plateforme internationale de la criminalité dans laquelle

l'individu peut s'immiscer en tout anonymat, effectuer une multitude de crimes et délits et communiquer avec ses associés en toute discrétion. Cet ensemble de facilités fait d'Internet un lieu à la fois propice au crime isolé, tel le hacker « *historique* » qui s'introduit illégalement sur un site web protégé, ou au crime organisé commis par des organisations internationales dotées d'une logistique hors norme et de ramifications indécelables.

I. Des difficultés pour établir un profil type de cyberdélinquant

L'analyse des actes de criminalité « *classique* » montre qu'il est possible d'établir finement un profil de corrélation entre crime et criminel. En revanche dans l'espace cyber, récent et marqué par l'immédiateté, l'anonymat et la dématérialisation, ce système de corrélation semble être dépassé.
Néanmoins, la recherche des profils des cyberdélinquants est un enjeu majeur, notamment en ce qui concerne les enquêtes judiciaires. Ce travail d'identification constitue une réelle difficulté en raison des caractéristiques d'Internet mais aussi du fait qu'il existe une multitude de profils.
Les retours d'expériences concernant les cybercriminels qui ont pu être identifiés sont peu nombreux. Ils démontrent toutefois qu'il est impossible d'obtenir un schéma général des profils. En France, les individus mis en cause par l'OCLCTIC[2], agissant et se trouvant sur le territoire national, se révèlent être des programmeurs ou de jeunes passionnés d'informatique se trouvant en marge du monde social. Ils ont un quotient intellectuel supérieur à la moyenne et sont capables d'aller chercher les renseignements sur Internet afin de programmer des virus. Ils agissent principalement pour l'appât du gain et le défi technologique.
Cela diverge légèrement des ébauches de profils constatés au sein de l'ex-bloc soviétique. En effet, le profil abstrait du jeune russe qui pirate dans sa cave doit être abandonné. S'il s'agit, comme en France, d'individus relativement jeunes, nés en moyenne entre 1980 et 1992, constituant une population instruite et passionnée par l'informatique, ils ne sont pas tous marginalisés. Beaucoup d'entre eux sont déjà chargés de famille et disposent de peu de ressources. Par ailleurs, les structures les employant sont souvent imaginées comme générant de gros revenus mais ce n'est pas la réalité. Les salaires mensuels pour les plus nombreux varient autour de 500 $.
Le cas d'une organisation criminelle utilisant des Botnets met en exergue la capacité de groupes criminels classiques à utiliser Internet à leur profit en recrutant des spécialistes dans de multiples domaines (développeurs, serveurs, loueurs de temps, « *trafeur* », blanchisseurs…). Il est alors possible d'assister à la naissance de groupes se formant ponctuellement pour des durées ou des actions limitées. Des acteurs s'organisent en formant des sociétés pour essayer d'obtenir une « *vitrine* » et vendre des services (hébergeurs, prestataire Internet…).

2 - OCLCTIC : Office central de lutte contre la criminalité liée aux technologies de l'informatique et de la communication.

II. Que faire face à l'internationalisation de la cyberdélinquance ?

La disparition des frontières au sein du cyberespace fait rapidement apparaître des problématiques de coopération internationale. Effectivement, le but est d'aller au plus vite à la source des menaces. Il est donc indispensable d'organiser une coopération et une veille efficaces

à l'encontre des personnes capables de diffuser cette menace.
A cet effet, des pistes de travaux existent dans le cadre du G8 / G20. Des points de contact unique ont pu ainsi être identifiés et communiqués à l'ensemble des partenaires. Cela permet de figer sous le signe de l'urgence une situation et de geler des données techniques. Les informations peuvent alors être transmises au pays demandeur dans le cadre d'une demande de coopération.
Un rapport récent de l'Institut inter-régional de recherche des Nations unies sur la criminalité et la justice (UNICRI) fait le constat d'un manque de recherches approfondies sur le profil des cybercriminels (motivations, en fonction des pays, cibles attractives ou comme cyberparadis, coût et formalités d'hébergement, coût de la vie, etc...). Il devrait entraîner une réaction de la part de la communauté internationale et donner l'élan à un véritable travail de fond sur le sujet.
La France est considérée comme un grand pays d'Internet, disposant notamment d'hébergeurs majeurs. Elle est régulièrement utilisée comme étape, rebond ou base arrière par les cyberdélinquants. Sans victime ni auteur sur son territoire, notre pays a une réelle difficulté à mettre en place une politique de réaction optimale pour identifier et fournir les informations. En conséquence, de nouveaux mécanismes doivent être trouvés dans la coopération internationale.

A5 - Cybersécurité et continuité des services publics

Intervenants :

- Christian Chocquet : Préfet délégué pour la Défense et la sécurité, zone de défense Nord,
- Matthieu Gillon : Responsable sécurité des systèmes d'informations, Préfecture Nord – Pas de Calais,
- Johane Protin : Responsable de la sécurité des Systèmes d'Information, Correspondant informatique et libertés, Conseil général des hauts-de-Seine,
- Richard Olszewski, Directeur Général, Securban,
- Emmanuel Besson, Directeur technique et co-fondateur de 6Cure.

Résumé des interventions :

La continuité des services publics en situation de crise est un principe à valeur constitutionnelle. La croissance des procédures numériques et les nouveaux comportements des citoyens génèrent des attentes spécifiques en terme de rapidité et de fiabilité dans les services rendus. Les notions de temps et d'espace sont abolis et les sécurités administratives traditionnelles ne sont plus opérationnelles. La multiplication des mises en réseaux entre des opérateurs publics avec des niveaux de fragilité et d'intérêt stratégique oblige tous les acteurs à une redéfinition des prédateurs potentiels. La mise en place de tout système ne peut s'envisager qu'avec une réflexion des process de sécurité de la part des collectivités et de l'ensemble des collaborateurs. Avec l'intervention des opérateurs privés, le partage des données et les conditions dans lesquelles celles-ci seront réutilisées, elles sont des éléments clés dans la chaîne de sécurité. Le cahier des charges, la définition des besoins, l'identification des acteurs en terme de sous traitance, la traçabilité du service de création et de maintenance, les procédures de contrôle sont les conditions à définir pour empêcher des prédateurs potentiels. Le développement de l'administration e-numérique modèle le territoire. Les collectivités sont garantes d'une culture du service public. L'État est opérateur de solutions sur la veille cybercriminelle en s'appuyant sur les réseaux d'expertise coordonnés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), en favorisant la formation des services enquêteurs, enfin en s'appuyant sur le tissus industriel du territoire national.

I. Les problématiques

La continuité des services publics est un principe à valeur constitutionnelle. C'est aussi un enjeux aux regard des droits sociaux et des devoirs de l'État. En cas de pandémie ou de crise, les services publics doivent être en mesure de respecter leurs obligations en temps et en lieu.

Le développement des procédures numériques et la multiplication des portails virtuels impactent de plus en plus de services à tous les niveaux de l'administration du pays. L'attente du public est tout autant démultipliée par les nouvelles pratiques sociétales et technologiques. Le parc de la téléphonie individuelle et des ordinateurs concerne toutes les classes socioprofessionnelles. Le développement continu de la technologie efface les notions de temps et d'espace et justifie l'obligation d'un service instantané, délocalisé et individualisé. Le public attend des services de l'État et des collectivités d'être réactifs et de produire une information fiable et sécurisée. Les courbes de croissances des intrusions en cybersécurité suivent les mêmes tendances. L'accroissement des connexions favorise aussi la multiplication de mise en réseaux d'interlocuteurs publics avec des niveaux de vulnérabilité et de vigilance différents. Pour les administrations centrales et stratégiques, les prédateurs sont identifiés et les procédures de sécurité sont performantes. En revanche, à l'aune du territoire, de nombreux acteurs publics, notamment les collectivités, ignorent l'existence de prédateurs et les verrous de sécurité sont faibles. La complexité des technologies, le développement de réseaux, la qualification des demandes impliquent l'intervention croisée des opérateurs publics et privés, ce qui accentue la vulnérabilité de l'e-administration.

II. Des solutions

La création d'un outil numérique doit se penser et se construire avec un système de sécurité opérationnel. La croissance et la multiplication des connexions entre services publics augmentent les opportunités d'accès des prédateurs. La fragilité du système réside surtout auprès des administrations qui sous-estiment le danger au regard de leur activité non stratégique. Les acteurs historiques, les réseaux de l'État, vont devoir penser une politique de sécurité hors de leurs cadres. La connexion des différents réseaux de l'État avec des collectivités locales ou des services décentralisés nécessite un travail de sensibilisation des acteurs publics aux enjeux de la cybercriminalité. Les réseaux sont fragilisés par des personnels qui ne maîtrisent pas le concept de sécurité tant dans la gestion de son architecture que du fait de mauvaises pratiques persistantes.

La prospective d'un système numérique nécessite pour la collectivité d'être le plus en amont possible pour englober tous les enjeux, la finalité, les besoins et les risques pour elle-même et les bénéficiaires. Les services de sécurité informatique ne sont pas les seuls interlocuteurs lors de cette phase de mise en confiance numérique avec des partenaires à qui l'on va ouvrir le réseau. L'ensemble du maillage informatique et des acteurs doit être impliqué. La collectivité doit piloter son projet dans sa structure et au travers des différents acteurs. La complexité des services numériques rend nécessaire l'externalisation et l'appel aux entreprises privées. Il est important de définir contractuellement comment et à qui on va dévoiler les modes de gestion et les éléments environnementaux qui spécifient le réseau. La rédaction des cahiers des charges pour les marchés publics doit traduire cette

communication, stipuler les clauses de sécurité, les conditions de suivi et la traçabilité des entreprises sous-traitantes. Les collectivités doivent aussi penser à adosser au cahier des charges des procédures de contrôle et de suivi.
Le développement de l'administration numérique modèle le devenir du territoire. Les responsables des collectivités sont responsables de l'aménagement numérique du territoire. Ils sont les artisans de la confiance numérique et d'une éthique de l'e-administration qu'ils doivent faire connaître et respecter par les techniciens. Les collectivités sont garantes et initiatrices d'une culture du service public qu'il est nécessaire d'apporter aux partenaires privés pour une modélisation cohérente. Bien qu'il n'y ait pas de gouvernance générale en France des services de sécurité, les collectivités devraient trouver auprès de l'État des mesures directrices nécessaires à leur prérogatives de garant des droits du citoyens et des moyens de gouvernance des systèmes de sécurité.
L'État est aussi tributaire des prestataires de services privés et certains leviers de l'environnement de l'e-administration échappent à la maîtrise publique. Mais il reste en mesure d'apporter des réponses en terme de gouvernance globale. Il doit renforcer l'aspect défensif des réseaux d'expertise et de veille, coordonnés au niveau national par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et des hauts fonctionnaires de la Défense et des ministères concernés. Les services enquêteurs doivent être mieux formés à la cybercriminalité afin de valoriser une veille des indicateurs de fragilité ou de synergies mises en place par des cybercriminels à l'encontre des intérêts nationaux. La veille numérique est aussi tributaire des pôles recherche et développement développés par l'État. Cette veille d'intelligence économique est à la mesure du pays. Au même titre que les grandes entreprises, les petites entreprises participent au maillage numérique du territoire.
A l'échelle européenne, l'État devrait pouvoir s'appuyer sur un corpus législatif commun en cours d'élaboration.

A6 - Nouvelles formes de conflictualités dans le cyberespace

Intervenants :

- Didier Danet : Responsable du pôle Action Globale et Forces Terrestres – Centre de recherches des écoles de Saint-Cyr Coëtquidan,
- Olivier Kempf : Maître de conférences à Sciences Po – Alliance géostratégique,
- Stéphane Dosse : Lieutenant-colonel, Ministère de la défense,
- Daniel Ventre : Ingénieur CNRS, titulaire de la chaire Cyberdéfense et cybersécurité – Écoles de Saint-Cyr Coëtquidan – Sogeti - Thales,
- Oriane Barat-Ginies, Juriste en droit international – État-Major des Armées.

Résumé des interventions :

Le développement massif ces dernières décennies de l'informatique et des nouvelles technologies a donné naissance à un nouvel espace d'échanges sociaux et économiques en constante expansion. En son sein a pris forme une nouvelle typologie de conflictualité polymorphe qui peut aussi bien toucher les sphères personnelles et familiales qu'industrielles, commerciales et étatiques. Une réelle problématique existe quant à la qualification des cyberconflits et leur interprétation au regard du droit international. Il ne s'agit pas de dégager un nouveau droit ex nihilo mais d'adapter le droit existant à ces nouvelles formes d'agressions.

La maîtrise de l'information et des communications a très tôt pris une place prépondérante que ce soit au niveau commercial, industriel ou sur le terrain de la Défense. Très rapidement, les différents acteurs présents dans le cyberespace ont pris conscience de l'importance de ce vecteur et des risques qui en découlaient. La technicité des actions tendant à paralyser ou à prendre le contrôle des moyens de communication évoluant à un rythme effréné, il s'agit de s'adapter rapidement et de faire évoluer les dispositifs techniques mais aussi législatifs afin d'éviter le développement d'un régime d'impunité.

I- Le cyberespace : lieu d'expression d'une nouvelle conflictualité

Un constat se doit d'être établi quant à l'universalité du monde cyber. La multiplication des ordinateurs, smartphones et systèmes informatiques de tout genre touche la quasi-totalité de la population mondiale, ne serait-ce que dans les gestes les plus simples de la vie quotidienne. En effet, une simple carte bancaire fait bel et bien partie de ce monde cyber.

La multiplication des acteurs est aussi un point

essentiel à souligner. Pas moins de 7 milliards de téléphones mobiles sont aujourd'hui en service sur la planète. L'individu est désormais un acteur stratégique. Si auparavant, il déléguait sa part de souveraineté individuelle, le cyberespace lui a rendu possible l'exploitation de sa propre part de souveraineté.
Le phénomène d'inattribution des actions commises sur le cyberespace renforce cette possibilité donnée aux individus. En effet, on peut y agir de façon opaque et cachée, ce qui donne un sentiment d'impunité. Par extension, une comparaison peut être faite avec la dissuasion nucléaire : on connait le détenteur de l'arme et les effets que l'usage de celle-ci pourrait occasionner. Dans le monde cyber, aucun de ces deux critères n'est rempli et il est très difficile d'identifier l'auteur d'une attaque (Estonie 2007, Stuxnet découvert en 2010). La liberté de manœuvre qu'il procure a aussi une grande importance pour les États qui souhaiteraient utiliser le monde cyber dans leur stratégie de défense. Aujourd'hui, une action informatique connaît encore beaucoup moins de retentissement médiatique qu'un bombardement aérien. La stratégie du Président Obama dans la mise en œuvre de drones, de manœuvres informatiques défensive et offensive en est une bonne illustration.
Enfin, la grande nouveauté apportée par le cyberespace dans le domaine des conflits est la création d'un régime de l'offensive. Auparavant, le fait d'avoir connu la guerre totale mais aussi de l'existence la dissuasion nucléaire donnaient lieu à l'application d'un régime défensif ayant pour culte la notion de légitime défense. Ce temps est révolu.

II. L'adaptation du cadre juridique existant

Un désaccord subsiste sur la question des cyberconflits. Peut-on réellement parler de cyberguerre ?
S'il existe un droit international des conflits armés et une définition juridique de la guerre, il n'en est rien quant à la notion de cyberguerre. L'absence d'une définition pour ce vocable en droit international est fondamentale. En effet, si aucun texte ne définit la cyberguerre et les éléments qui la composent, aucun cadre juridique ne peut être appliqué. On pourrait définire le jus ad bellum par un faisceau d'indices reprenant la sévérité des dommages infligés, le degré de pénétration dans les systèmes et les effets connus dans le temps. En droit international, l'agression armée est clairement définie et elle entraîne le droit pour l'État qui en est victime, d'agir en légitime défense. Il est en effet difficile de caractériser une attaque informatique au regard d'une réponse en situation de légitime défense tout en prenant en compte les critères de la temporalité ou encore de la proportionnalité de la réponse à l'attaque. L'agression informatique n'est pas définie par le droit international. Sur la notion de jus in bello, les conflits armés internationaux et conflits armés non-internationaux sont clairement définis, or les cyberattaques n'engendrent pas de pertes humaines directes. En 2008, le conflit entre la Géorgie et la Russie a engendré des pertes humaines et des cyberattaques ont été utilisées lors de ce conflit. La cyberguerre peut-elle donc être considérée comme une guerre à part entière ou n'est-elle pas qu'un moyen de la guerre ?
Les mêmes questions peuvent être posées sur la question du cyberterrorisme : un groupe de hackers peut-il être considéré comme une

formation organisée alors que les hackers n'agissent pas toujours avec des revendications politiques, religieuses ?
Des arguments militent en faveur de la reconnaissance de l'existence d'une vraie notion de cyberguerre : elle ne serait qu'une adaptation des moyens actuels aux principes tactiques pluriséculaires. En effet, c'est à la fin du XIXe siècle qu'est apparue, concomitamment à leur développement, une géopolitique des moyens de communication et des câbles. La première véritable illustration en a été la seconde guerre des Boers qui a eu lieu en Afrique du Sud de 1899 à 1902. Ensuite, sont rapidement apparues les notions de brouillage, de localisation puis de cryptoanalyse ou encore de cryptographie durant la seconde guerre mondiale. On ne peut parler de cyberguerre à cette époque mais on constate que les armées ont su, dès leur apparition, utiliser les systèmes de communications pour peser lourdement sur l'issue des conflits. De plus, si les attaques cybernétiques ne donnent pas lieu à des pertes directes de vies humaines, le temps et l'argent perdus par les États victimes de ces attaques ne suffiraient-ils pas à constituer un préjudice justifiant une action en situation de légitime défense ?

Il ressort de cette approche que les états doivent continuer à s'adapter à ces nouvelles menaces. Il n'existe pas de réel vide juridique sur la question mais plutôt une grande difficulté à adapter les normes existantes au domaine cyber. Les États doivent tenter de transcrire au mieux les normes internationales au regard des conflits armés pour que naisse progressivement un véritable droit des conflits informatiques.

A7 - Gouvernance du cyberespace

Intervenants :

- Loïc Damilaville : Adjoint au directeur général Afnic,
- Jean-François Blarel : Secrétaire général adjoint, ministère des Affaires étrangères,
- Bertrand de la Chapelle : Membre du conseil d'administration de l'ICANN, directeur du projet « Internet et juridication » à l'académie diplomatique internationale,
- Nemanja Malisevic : Cyber security officer, OSCE ,
- Jérémie Zimmermann : Co-fondateur et porte-aprole, La Quadrature du Net.

Résumé des interventions :

Les problématiques de gouvernance du cyberespace sont très complexes et démontrent des positions étatiques parfois contradictoires. Suscitant de fortes convoitises, le cyberespace est devenu un enjeu pour les États et les organisations internationales qui se livrent à une lutte âpre. Les mécanismes de la gouvernance doivent évoluer pour arriver vers un équilibre en donnant à l'internaute sa pleine et juste part.

La gouvernance de l'Internet ? Nul n'est en mesure d'en donner une définition claire alors que des milliers de personnes y participent – directement ou indirectement - depuis plusieurs années. D'une manière globale, la gouvernance de l'Internet désigne les principes et règles qui modèlent et modulent l'évolution et l'usage d'Internet et qu'élaborent et appliquent les acteurs (États, secteur privé, société civile). Il faut distinguer deux aspects d'essence interactive : le gouvernement de l'Internet (avec des enjeux politiques) et la gestion de l'Internet (avec les problèmes techniques).
De fait, les choix techniques résultent souvent de la vision « *politique* » de la solution à apporter et, parallèlement, l'environnement politique est conditionné par certains choix techniques. Cette interpénétration suscite de nombreuses interrogations.

I. Les gouvernements et le cyberespace : une lutte âpre

Internet est un puissant facteur de croissance économique (numérique), doublé d'un espace de liberté et de démocratie (rôle prépondérant de l'Internet lors du Printemps arabe par exemple). Internet peut aussi devenir le théâtre d'action de personnages sans scrupules, avançant à couvert pour mener leurs attaques informatiques ou se livrer à la cybercriminalité.
Si l'intervention de l'État dans des secteurs traditionnels (protection du citoyen, ordre public, préservation des systèmes informatiques vitaux pour la Nation) est parfaitement légitime, son implication dans la gestion du cyberespace demeure néanmoins d'application délicate car, d'une certaine manière, il s'agit ni plus ni moins d'une remise en cause du principe de territorialité. Suscitant une forte convoitise, le cyberespace

est devenu l'enjeu de « *manœuvres diplomatiques* », au même titre que l'étaient en leur temps le domaine maritime ou l'espace extra-atmosphérique. On assiste ainsi à une volonté de plus en plus marquée de juguler Internet dans un carcan intergouvernemental par le jeu d'alliances et de liens politiques. Dans ce débat sur le cyberespace, se dégagent globalement deux positions :

- celle des USA et de l'Europe qui prônent une approche « *multipartite* » du cyberespace[1] : les États ne sont pas les seuls acteurs sur Internet et l'espace est partagé avec la société civile, les associations, les particuliers... Le constat qui se dégage est qu'il faut renforcer la cybersécurité mais veiller à ce que les contrôles ne limitent la liberté d'expression ;

- celle soutenue notamment par la Russie et la Chine qui partent du principe qu'il revient aux États de mettre en place un instrument juridique plus contraignant. Les pays qui hésitent à prendre parti (groupe des « *77* ») font l'objet d'opérations de séduction (fourniture de technologies clef en main) pour les attirer. La Chine et la Russie préconisent un transfert de gouvernance à un organisme intergouvernemental.

Ces approches nettement différenciées ont animé les débats à l'occasion de la conférence internationale des télécommunications à Dubaï, en décembre 2012, où la lutte d'influence quant à la place d'Internet dans la société est apparue au grand jour.

1 - Sans toutefois faire preuve d'angélisme puisque aujourd'hui les USA sont les seuls à contrôler techniquement le système racine et peu enclins à le partager.

II. Des divergences, mais aussi des intérêts communs

La sécurité des systèmes d'information et de communication ne peut pas être traitée individuellement. A cet égard, l'organisation pour la sécurité et la coopération en Europe (OSCE) se concentre sur le développement pour la confiance des technologies de communication et de l'informatique. Cette confiance est capitale et constitue un grand défi pour les communautés internationales. Les États de l'OSCE tentent de prévenir les attaques pirates par la mise en place de règles cybernétiques mais, à ce jour, aucun accord n'a pu être finalisé car les décisions sont prises par consensus (56 États membres). La route pour arriver à un accord est difficile car chaque État définit ses priorités et il faut aplanir les nombreuses divergences. Il y a cependant un intérêt commun des États pour renforcer la sécurité. Les pistes pour y arriver existent : promotion des négociations bilatérales et internationales, « approche ascendante » par une prise en compte des positions dites du plus petit dénominateur commun. L'instauration d'une confiance sera un facteur d'avancées en la matière. Ces négociations s'avèrent complexes mais l'intérêt des États étant évident, on ne peut que progresser.

III. Internet, zone de non-droit ou de sur-droit ?

Le droit des libertés sur Internet est fondamental pour informer le citoyen et lui permettre d'agir. Existe-t-il une alternative à la gouvernance de l'Internet ? Le débat doit être le plus large possible, en prenant en compte aussi bien les

paramètres techniques qu'humains et sociaux (les usages). Toute décision technique a un impact politique (ex : la force des noms de domaine). Face à un choix de société, deux tendances se dégagent :

- l'appropriation exclusive basée sur le contrôle reçoit des échos divergents dans des politiques publiques (mesures législatives ou politiques à l'exemple d'Hadopi ; contrôle des communications ; outils de la censure…) ;
- le modèle d'ouverture avec les maîtres mots de partage, d'universalité, de potentialité d'accès, d'ouverture, de neutralité. Les gouvernement doivent prendre les mesures pour protéger les universalités (données personnelles et privées).

Internet est un bien commun, il appartient aussi aux citoyens, et par conséquent relève de la responsabilité collective. Le citoyen peut peser sur les décisions ; ainsi une levée de boucliers contre le projet d'accord commercial anti-contrefaçon, négocié secrètement entre une quarantaine d'États, a parfaitement illustré l'universalité d'Internet et de ses acteurs.

Espace transfrontalier par nature, Internet est, par voie de conséquence, soumis à autant de juridictions qu'il y a de pays concernés (localisation des serveurs, utilisateurs, pays d'accueil…) Dès qu'une plateforme se situe dans une juridiction particulière, elle se verra appliquer la loi du territoire géographique dans lequel elle se trouve. Dès lors, il serait plus juste d'évoquer « *les gouvernances* » des cyberespaces, car il y a une collection d'espaces partagés (privé, semi-public, public).

Par ailleurs, l'architecture de l'Internet reposant sur différentes couches qui ne sont pas physiquement liées (couche physique, liaison, réseau, transport), la tentation est grande de voir des gouvernements utiliser la couche logique pour traiter aussi des contenus (notamment en appliquant les souverainetés nationales aux opérateurs installés dans leur pays) ; il y a un risque de phénomène d'extra-territorialisation auquel il faut veiller car la neutralité de la couche logique doit être préservée.

Cette course aux armements juridictionnels est source de tensions, liée à l'incertitude sur le droit applicable, aussi bien pour les gouvernements que les entreprises ou les utilisateurs.

2 - On est passé en l'espace de deux décennies de 10 000 à 2,3 milliards d'internautes

Dans une économie de systèmes et d'acteurs qui a le mérite de fonctionner[2], un contexte général d'éclatement du rôle des États-nations issus des traités de Westphalie et une montée en puissance d'autres sources, il convient de trouver de nouveaux équilibres entre les parties. En effet, on ne peut imaginer une gouvernance de l'Internet sans les gouvernements, de même qu'une gouvernance où ils seraient "seuls aux commandes" paraît assez illusoire.

La présence de multi-acteurs constitue un levier permettant de trouver des points d'équilibre[3]. Il faut développer la gouvernance sur l'Internet en accroissant les mécanismes inter-acteurs et redonner toute sa part au citoyen.

3 - L'agenda de Tunis pour la société de l'information a défini en novembre 2005 les principes selon lesquels l'Internet est devenu une ressource publique mondiale et que sa gouvernance devrait s'opérer de façon multi-latérale, transparente et démocratique avec la pleine participation des États, du secteur privé, de la société civile et des organisations internationales.

A8 - La modernisation des moyens de prévention et d'investigation dédiés au traitement des infractions cybercriminelles

Intervenants :

- Joël Ferry : Colonel, Direction générale de la Gendarmerie nationale,
- Éric Freyssinet : Lieutenant-colonel de gendarmerie, STRJD/DLCC ,
- Philippe Joliot : Expert près de la Cour d'Appel de Nancy, Président de TRACIP,
- Anne Souvira : Commissaire divisionnaire, BEFTI, Préfecture de Police de Paris.

Résumé des interventions :

L'évolution des technologies de l'information et de la communication impose aux différents acteurs de l'enquête judiciaire d'agir sur le plan national et international en parfaite synergie pour assurer le recueil et le traitement des preuves numériques. Des mesures efficaces sont déjà mises en œuvre. Toutefois, pour faire face à l'évolution des moyens numériques dans un univers international ouvert, des mesures nouvelles et innovantes doivent être recherchées.

I. Les instruments de prévention et d'investigation concernent les moyens juridiques et techniques

Le recueil de traces ou indices discutés contradictoirement vont constituer devant le juge un faisceau de preuves susceptible de conduire à la culpabilité du mis en cause. Ces éléments vont être obtenus sur la scène de crime lors des constatations par les enquêteurs spécialisés en technologies numériques. L'enquêteur devra respecter un protocole afin de ne pas dénaturer ce qui pourra devenir un élément de preuve. L'expert aura des contraintes identiques.

En dehors de la scène de crime, d'autres mesures procédurales pourront être mises en œuvre afin d'obtenir des éléments qui deviendront des éléments de preuve comme par exemple les dispositifs d'interception ou récemment de sonorisation autorisés par la loi afin de permettre les interceptions en matière de voix sur IP (skype notamment).

En matière de prévention, on rappellera le dispositif législatif autorisant l'exercice de cyberpatrouilles visant à détecter les échanges illégaux en matière de jeux en ligne, terrorisme

et pédophilie.
L'examen d'un support pourra être mené pour connaître les informations stockées comme, par exemple, l'existence d'images pédophiles sur un ordinateur ou encore les derniers appels contenus sur un téléphone portable, ou les dernières transactions d'une carte bancaire.
Toutefois, depuis une dizaine d'années, la tâche est devenue plus difficile, car le volume et la nature des informations à analyser sont de plus en plus importants et complexes. Des moyens techniques ont été progressivement développés, comme les logiciels permettant de révéler des informations après l'effacement des données sur un disque dur, ou encore des bases de données stockant des signatures numériques d'images pédophiles permettant de détecter sur des machines des indices durant le temps de la garde à vue d'une personne.
Avec la convergence des systèmes (ordinateurs et téléphones portables qui constituent de mini-ordinateurs) notamment en mobilité, la multiplication des moyens comportant des systèmes numériques (voitures, consoles de jeux dotées de messageries, les cartes à mémoire de toute nature, caméscopes…), l'examen des moyens numériques est rendu nécessaire, quelle que soit la nature des infractions commises. La tâche est donc rude.

II. Face à l'évolution des moyens numériques dans un univers international des mesures nouvelles et innovantes doivent être recherchées

L'évolution des technologies numériques va rendre encore plus difficile la récupération de la preuve. Des adaptations du droit et des moyens d'investigation seront de nouveau nécessaires.
Avec la norme IPV6, le web des objets communicants, l'utilisation à terme de la troisième dimension, l'internationalisation des données stockées dans le « *cloud computing* » sera la règle. Mais personne ne saura exactement où elles se trouvent. Il existe cependant des technologies pour traiter les informations stockées dans le cloud mais le déploiement des logiciels doit être réalisé en partenariat avec les hébergeurs français et étrangers. Un partenariat public/privé devrait donc être envisagé tout en considérant que plus de la moitié des hébergeurs dans le monde se situent aux USA et, en Roumanie, pour l'Europe.

- En attendant, pour obtenir les informations recherchées, si les données s'avèrent être stockées à l'étranger, il sera toujours possible d'invoquer la convention de Budapest pour les obtenir facilement. Cependant cette convention n'a été signée et ratifiée que par un nombre limité de Nations essentiellement européennes. Pour les autres États, il convient de mettre en œuvre l'entraide judiciaire en matière pénale traditionnelle en appliquant une convention bilatérale si elle existe, et, à défaut, en passant par le canal diplomatique. D'une manière générale, les délais d'exécution sont souvent trop longs, ce qui rend inopérant la demande et limite la résolution de l'enquête. Aussi, il serait nécessaire d'élargir les adhésions à la convention de Budapest à d'autres États non européens. Il conviendrait également de réfléchir à la façon d'obtenir les éléments de preuves à l'étranger d'une manière plus rapide en améliorant notamment les mécanismes de coopérations judiciaires dans le respect du principe de souveraineté des États.

- Une autre piste consisterait

à améliorer les relations institutionnelles avec les grandes sociétés d'hébergement internationales comme Google, Yahoo ou Twitter. Il conviendrait en outre de développer de nouveaux outils, de « *reverse ingénierie* » pour découvrir les traces laissées sur les supports numériques.
Le « *web profond* » fait également partie des espaces non contrôlés du web où des efforts doivent encore être consentis dans l'intérêt de la sécurité des personnes, des entreprises et des États. Des équipes d'enquêteurs devraient être dédiées à chaque couche du web, alors que des outils spécifiques performants n'existent pas à ce jour.
Pour anticiper les besoins face à l'évolution des services du web, il conviendra de définir rapidement des politiques de recherche et de développement avec les laboratoires du secteur public ou privé. Des conventions allant dans ce sens doivent être dés à présent envisagées.

III. La formation des acteurs de la chaine pénale demeure plus que jamais une nécessité

Enquêteurs et experts remplissent des missions différentes mais complémentaires. Dans le principe, les premiers peuvent requérir en cas de nécessité l'intervention des seconds pour récupérer des éléments de preuve. Toutefois, le rôle de l'expert fait l'objet d'un recentrage. Maintenant que les enquêteurs spécialisés maitrisent les actes techniques complexes durant la phase de police judiciaire, les experts interviennent pratiquement exclusivement durant la phase de l'instruction. Au regard de leurs missions, de l'évolution des technologies numériques et des difficultés rencontrées identiques, enquêteurs spécialisés et experts partagent leurs connaissances. Les experts vont tenter de développer leurs propres outils d'investigation. Pour cela, ils vont se rapprocher de l'université (Neuchâtel, Nancy). Les laboratoires d'expertises collaborent également entre-eux et échangent leurs expériences. A terme, avec l'évolution des systèmes, ils devront se spécialiser dans des domaines précis en raison de la complexité des supports et des services proposés (carte à puce, ordinateur, téléphones…).
Il existe également une véritable volonté de formation des enquêteurs spécialisés sur le plan national et international. En France, les différents services d'enquête coopèrent pour permettre des échanges d'expérience et de bonnes pratiques. Le dispositif européen 2centre est destiné à donner aux enquêteurs spécialisés en technologie numérique de l'Union européenne une formation de haut niveau analogue. En France cette formation s'appuie sur le monde académique.
Le magistrat dans le traitement de la preuve devra de plus en plus s'intéresser aux questions techniques et pour cela bénéficier d'une formation pluridisciplinaire dans le domaine numérique. Il devra également s'appuyer sur une politique pénale clairement définie.

A9 - Cyberespace et contrefaçon

Intervenants :

- Corinne Champagner-Katz : Avocate au barreau de Paris, CCK Avocats,
- Luc Strohmann : Responsable cyberdouane, Direction nationale du renseignement et des enquêtes douanières (DNRED), Ministère de l'économie et des finances,
- Éric Przyswa : Chercheur associé Mines ParisTech, Centre de recherche sur les Risques et les Crises (CRC),
- Nadia Lamrhari : Juriste en propriété intellectuelle et nouvelles technologies, Priceminister,
- Thierry Bourret : Colonel, Chef de bureau, Direction générale de la Gendarmerie nationale.

Résumé des interventions :

La contrefaçon n'est pas née avec Internet mais celui-ci l'a largement facilité en « *dématérialisant* » la plupart des transactions, en simplifiant la chaîne logistique et en créant une distance entre le produit et le consommateur. Quelle est l'ampleur du phénomène sur Internet ? Quel impact sur la compétitivité de nos entreprises et comment peuvent elles se protéger ?

I. Les problématiques

La contrefaçon représente une atteinte aux droits de propriété intellectuelle qui entraine un préjudice protéiforme pour les entreprises. Il en va directement de la captation des parts de marchés pour l'entreprise victime et de la diminution de son chiffre d'affaires avec toutes les conséquences économiques que cela représente : des pertes d'emploi et de recettes fiscales.

Les faits de contrefaçon concernent désormais tous les secteurs de l'économie et ne se limitent plus uniquement à l'industrie du luxe. Les entreprises qui souhaitent se développer à l'international doivent obligatoirement se protéger dans les pays concernés mais elles vont rencontrer des écueils dus au fait de l'absence de législation universelle. L'autre difficulté réside dans le développement commercial par Internet et les sites de vente à distance. La mise en ligne d'un site officiel, permettant de diffuser les produits, va obligatoirement créer un drain pour les contrefacteurs qui vont réaliser un site identique et vendre des contrefaçons en jetant un trouble dans l'esprit du consommateur.

Le cyberespace est un nouveau vecteur que les contrefacteurs ont très rapidement adopté. Il permet de proposer de multiples articles sans détenir de stock et de sensibiliser un maximum de clients à travers le monde. L'ensemble des possibilités offertes par Internet est utilisé : les petites annonces, les blogs, les sites et également les réseaux sociaux. L'adaptabilité des cyber-

contrefacteurs est permanente et l'arrivée massive des propositions de vente de contrefaçons sur des réseaux tels que Facebook ou Twitter le démontre.

II. Des solutions

La première action des entreprises doit consister à se protéger par le dépôt de leur marque, dessins ou modèles. Ces dépôts ne doivent pas se limiter à la France, même si l'objectif premier n'est pas le développement international. Il est primordial d'accompagner les TPE et les PME qui sont esseulées face à la problématique de la contrefaçon.
En cas de violation des droits de propriété intellectuelle, l'action civile est la solution la plus utilisée. Cette procédure consiste à rechercher la responsabilité du contrefacteur et à matérialiser les actes de contrefaçon. Après avoir recueilli les éléments, il existe en France une arme législative appelée « la saisie contrefaçon ». Il s'agit d'une action dérogatoire autorisée par un magistrat qui permet de mener une action de saisie avant tout débat contradictoire. La plus grande difficulté réside dans la détermination de la masse contrefaisante qui est essentielle lors du jugement.
La France possède un arsenal juridique important qui donne la possibilité aux titulaires de droit, outre l'action civile, de se tourner vers les services répressifs tels que les douanes, la gendarmerie ou la police nationale. Les douanes et la gendarmerie ont un service dédié à la cybercontrefaçon qui permet de détecter les ventes d'articles contrefaisants sur le net. Les deux structures travaillent en parfaite collaboration avec les titulaires de droits et leur action se concentre sur les flux financiers. Les saisies réalisées par les douanes en 2012 sur le fret-express représentent 1,4 millions d'articles sur un total de 4,6 millions.
Les prestataires de l'Internet jouent un rôle important dans la lutte contre la contrefaçon. Le site Priceminister, dont le fondement est basé sur le tiers de confiance, a adopté une stratégie de tolérance zéro. Une cellule spécifique anti-contrefaçon, regroupant 40 personnes, traite la validité des annonces mais également les retours clients en cas de vente de contrefaçon. Le vecteur Internet est devenu la principale problématique des titulaires de droit. Une coopération avec les services de l'État est nécessaire pour lutter efficacement contre ce fléau. Des avancées législatives sont nécessaires mais la mobilisation des compétences et la formation des entreprises sur les risques encourus restent la clé de voute de la réussite

A10 - La cybersécurité des systèmes industriels

Intervenants :

- Corinne Champagner-Katz : Avocate au barreau de Paris, CCK Avocats,
- Luc Strohmann : Responsable cyberdouane, Direction nationale du renseignement et des enquêtes douanières (DNRED), Ministère de l'économie et des finances,
- Éric Przyswa : Chercheur associé Mines ParisTech, Centre de recherche sur les Risques et les Crises (CRC),
- Nadia Lamrhari : Juriste en propriété intellectuelle et nouvelles technologies, Priceminister,
- Thierry Bourret : Colonel, Chef de bureau, Direction générale de la Gendarmerie nationale.

Résumé des interventions :

La contrefaçon n'est pas née avec Internet mais celui-ci l'a largement facilitée en « dématérialisant » la plupart des transactions, en simplifiant la chaîne logistique et en créant une distance entre le produit et le consommateur. Quelle est l'ampleur du phénomène sur Internet ? Quel impact sur la compétitivité de nos entreprises et comment peuvent elles se protéger ?

I. Les problématiques

Elles résident dans l'existence d'un parc d'automatismes anciens conçus uniquement pour assurer la sûreté de fonctionnement qui relève de l'examen de la défaillance, alors que la sécurité relève de la recherche de la malveillance. Celle-ci, à l'origine, ne constituait pas auparavant une préoccupation car les automatismes étaient inscrits dans une architecture fermée, basée sur des ruptures protocolaires de protection. Lui ont succédé des structures IP qui offrent une large surface d'impact et de risques.

L'apparition d'une connectivité avec des interfaces grand public (Windows, Linux, etc…) et de processus de maintenance déportés ont ouvert les automatismes aux attaques. Les nouveaux systèmes doivent incorporer à la sûreté de fonctionnement la prise en compte d'une maintenance spécifique et une gestion du système d'information. Ils doivent intégrer le différentiel entre des automatismes d'une évolutivité au rythme décennal et des interfaces logicielles en constante évolution.

La prise de conscience a été tardive car les menaces étaient minorées. La problématique actuelle repose sur un manque d'informations et de culture connexe entre les informaticiens et les automaticiens. Il est impératif d'instaurer

une connexion entre ces deux logiques en visant une intégrité du système et des données. Le constructeur doit garantir l'intégrité du programme tandis que le traitement de cybersécurité conciliera l'intégrité des données et leur disponibilité avec les fonctionnalités de l'entreprise. A titre d'exemple, une porte automatique doit pouvoir s'ouvrir pour laisser passer les secours.
La définition des enjeux de la sécurité n'est pas du ressort de l'agent et des membres des SSI mais du plus haut niveau de décision de l'entreprise. Cet échelon doit endosser la responsabilité de l'analyse des risques résiduels.
On peut déplorer que la phase de l'audit et son pilotage ne dépassent pas le constat et on note que la politique des SSI est souvent abandonnée pour des raisons budgétaires.
Enfin nous devons distinguer obligatoirement la fonction d'audit et de contrôle.
La logique des coûts impose la recherche de solutions « sur étagères » et par conséquent l'alignement sur des standards. Les process sont affectés par des mises à jour des composants par « *patches* » pour assurer leur maturité industrielle. Une faiblesse logicielle reconnue du composant entraîne une fragilité généralisée des systèmes qui l'intègrent. Le client ne connaît pas la nature des patches. De fait, il n'a pas d'éligibilité et la qualité pour contrôler les patches implantés en maintenance. Souvent le client laisse en l'état le système tel qu'il a été livré.

II. Des solutions

Les solutions passent par l'incorporation contractuelle, lors de l'acquisition des automates et de leurs interfaces, de clauses relatives à des audits du système, au contrôle de ses mises à jour et à la cohérence des composants. Le cadre contractuel doit répertorier la disponibilité de l'information et du système. Les contrats de maintenance doivent être actés en conséquence.
Un politique d'audit interne doit être menée par une « *équipe structure* » externalisée de façon à confronter les pratiques des automaticiens et de leurs servants avec des personnels spécialisés dans la sécurité informatique. Les notes de service doivent être très pragmatiques et applicables.
Une intégration de l'interface entre les équipementiers et le client est indispensable. Toutefois, même si l'ANSSI a publié des guides, chaque contexte industriel et logiciel est spécifique. Ce qu'ont fait Alcatel et CISCO pour la téléphonie doit être un modèle pour les industriels.
Les certifications sont émergentes, mais les industriels doivent s'en inspirer pour organiser leurs produits autour d'une norme. La quasi totalité des normes sont issues d'entreprises américaines et d'ordre privé. Il est peu probable que l'on puisse acter une norme publique française ou européenne. Une certification par pays serait improductive. Il vaut mieux opter pour une certification de niveau mondial. Il faut s'inspirer des pratiques actuelles pour dégager une méthode de certification. Les méthodes privées américaines vont dans le bon sens du fait de leur appariement à un process industriel déjà maîtrisé en dehors d'un aspect marketing.
Ces normes nécessitent toutefois une vérification pour l'industriel qui veut les intégrer.
Il faut mener de manière volontariste un travail de sensibilisation des acteurs, de diagnostic, de détection des failles tout en restant confronté à des personnels qui ne maîtrisent pas le concepts de sécurité tant dans la gestion de son architecture que du fait de mauvaises pratiques persistantes.
Les formations doivent également concerner les pratiques défaillantes. Actuellement 90% des mots de passe correspondent à ceux des

appareils qui sont livrés.
Il est impératif pour les constructeurs d'informer le client sur les modalités de communication des automates, notamment ceux qui intègrent des serveurs Web. Il est en conséquence nécessaire d'engager des formations professionnelles. L'industriel-client doit avoir une parfaite connaissance du SCADA et de son évolution. Il doit connaître les modifications du système qui a été implanté initialement, celles qui ont affecté des sites déportés et qui font que les systèmes diffèrent en terme d'exploitation au sein d'un même ensemble d'informations.
La sûreté des processus peut emprunter la voie de la redondance des dispositifs d'acheminement des flux qui se révèle industriellement coûteux.
Il faut mieux mettre en place un chiffrement embarqué sur l'automate qui se révèlent efficace, bien qu'il engendre d'autres problématiques lors de la mise en œuvre.
Il se met en place de nouvelles plate-formes d'automatismes où le contrôle du code est pris en compte. C'est un avantage mais l'opération de contrôle doit être compatible avec des délais de réponse qui sont de l'ordre de la milliseconde.
Il faut prendre en compte dans les maintenances et les mesures de protection leur compatibilité avec l'architecture du système. A titre d'exemple, la mise à jour des 4000 RTU[1] français demande un temps considérable de l'ordre du mois. De même une solution antivirale se révèle mal adaptée du fait du contrôle et de la mise à jour des signatures, processus lent et par nature incomplet. On doit également prendre en compte la problématique des certificats volés même si elle est considérée comme marginale. C'est la raison essentielle pour laquelle la solution cryptée est la plus opportune.

1 - Remote Terminal Unit (RTU) : microprocesseur qui assure le lien entre diverses interfaces, notamment des systèmes de distribution de l'information ou des SCADA.

A11 - DRH et cybersécurité : quelles obligations pour l'employeur et le salarié ?

Intervenants :

- Florence Puybareau : journaliste,
- Blandine Poidevin : Avocate au Barreau de Lille, spécialisée en droit de l'Internet & Propriété Intellectuelle,
- Florent Chabaud : Ingénieur en chef de l'armement, Fonctionnaire à la sécurité des systèmes d'information (FSSI), Ministère de la défense,
- Sabine Marcellin : Juriste, Crédit Agricole Corporate & Investment, Forum des compétences.

Résumé des interventions :

Les entreprises, pour protéger leur patrimoine informationnel et la réputation des employeurs, doivent s'adapter à l'utilisation généralisée de l'outil informatique et d'Internet et mettre au point des procédés légaux de contrôle et de responsabilisation des salariés qui soient compris et admis de tous. Juristes, techniciens, responsables informatiques et de la sécurité des réseaux, services des ressources humaines ont chacun un rôle à jouer dans l'élaboration et l'application de la politique de sécurité de l'entreprise relative au comportement de ses salariés.

I. Les problématiques

La protection de la vie privée à l'intérieur de l'entreprise, qu'elle soit publique ou privée, est une obligation de l'employeur. En contrepartie, le salarié a obligation de loyauté et de confidentialité. L'utilisation, à titre personnel, de l'outil informatique, et plus particulièrement des réseaux sociaux mais aussi l'ouverture à leur nom de comptes par les entreprises, complexifient la situation.
D'une part, le salarié doit donc observer une retenue dans les propos qu'il peut être amené à échanger sur son employeur ou sur un produit et ne pas divulguer d'informations sensibles. D'autre part, l'employeur doit respecter ses engagements dans la protection des données personnelles et les dispositifs de surveillance mis en place. L'engagement, pour être efficace et avoir une valeur, doit être réciproque.
L'enjeu est de parvenir à trouver un équilibre satisfaisant entre la liberté d'expression du salarié d'un côté, reconnue et correspondant à une inévitable évolution de la société, et,

d'un autre côté, le contrôle de son image par l'entreprise. A cette difficulté s'ajoutent deux nouveaux constats : la demande de plus en plus fréquente faite par les entreprises aux salariés de relayer des messages au nom de l'entreprise sur leurs propres pages Facebook, comme par exemple des offres d'emploi, cette démarche étant jugée bénéfique pour l'image de l'organisation ; l'utilisation par les personnels de leurs propres équipements (ordinateurs, tablettes, smartphones personnels...) à des fins professionnelles, phénomène appelé BYOD (« bring your own device » qui signifie « prenez vos appareils personnels »). Ainsi, la frontière entre vie privée et vie professionnelle devient de plus en plus floue, de moins en moins aisée à déterminer, rendant plus complexe les éventuelles poursuites et sanctions, puisqu'un employeur ne peut faire procéder à des investigations sur un outil personnel.

Une autre problématique est celle des relations entre les différents services au sein de l'entreprise : la direction des ressources humaines (DRH), la direction des services informatiques (DSI), les responsables de la sécurité des systèmes d'information (RSSI) et les services juridiques et de contentieux. Les objectifs, les priorités et les langages des uns et des autres diffèrent. Une meilleure coopération est souhaitable car la sécurité relève de plusieurs métiers et ne peut dépendre efficacement des seuls RSSI.

C'est un droit en cours d'évolution et en construction, qui doit intégrer la dimension internationale du Web et répondre aux problématiques du salarié posté à l'étranger, de l'entreprise sous-traitée, du siège d'une société localisée dans un pays avec une règlementation différente.

II. Des solutions

Les chartes constituent le moyen le plus utilisé pour assurer la sécurité informatique des entreprises et encourager les bonnes pratiques : elles équivalent à un contrat entre le salarié et son employeur, signé par chacune des parties. Pour avoir une valeur juridique, donc être opposables et pouvoir servir de fondement à d'éventuelles sanctions, elles doivent satisfaire à un certain nombre de critères. Elles doivent se conformer aux législations et règlementations, françaises et européennes, et, à l'intérieur de ce cadre légal, être personnalisées pour répondre aux besoins spécifiques de chaque entreprise en terme de sécurité. Ces chartes rappellent les règles, issues du Code pénal, du droit de la presse, de la loi Godfrain, des textes relatifs à la protection des données personnelles, et mentionnent les outils de surveillance utilisés. Elle doivent être intégrées au règlement intérieur, négociées avec les partenaires sociaux, syndicats et instances paritaires, et portées à la connaissance des personnels, dans un souci de transparence. Des séances de formation dédiées peuvent être instaurées pour expliquer leur utilité et leur nécessité. Le but recherché est que les collaborateurs soient en mesure de se les approprier, qu'ils comprennent l'intérêt pour l'entreprise de mettre en place ces formes de contrôle et ne les considèrent pas comme une limitation à leur utilisation du système d'information. Ces chartes ont pour rôle de créer le droit positif dans l'entreprise. Il est donc primordial de faire attention au risque de leur obsolescence, de les vérifier régulièrement, de veiller à leur formulation de manière à édicter des règles générales qui puissent demeurer valides au-delà des évolutions technologiques. L'utilisation d'un identifiant et d'un mot de passe personnel

crée une obligation pour chaque salarié et permet, grâce au mécanisme de présomption induit, d'engager sa responsabilité. La Cour de cassation reconnaît la validité d'un licenciement fondé sur le non respect d'une charte informatique.
Les entreprises ont donc des moyens juridiques pour se protéger en amont et en aval et des procédures urgentes à leur disposition, telles les référés rapides. En effet, dans le cas où ces chartes ne suffisent pas à empêcher actes ou propos malveillants, des actions en justice peuvent être intentées. Les plus fréquentes actuellement le sont pour des infractions relatives au droit de la presse, notamment la diffamation, dans le cas de propos portant atteinte à l'honneur de la personne (morale ou physique) et pour l'infraction à l'article 1382 du Code civil dans le cas de la critique d'un produit. Des dernières décisions rendues, comme celle du 19 novembre 2010, on peut conclure que la responsabilité du salarié est reconnue quand le juge considère, après une analyse concrète des écrits échangés par le salarié sur Facebook que le statut est public. En effet, si le compte est visible par les « *amis des amis* », le licenciement se justifie en raison de l'ampleur de la diffusion.
Si les contenus incriminés sont stockés sur une infrastructure étrangère, ils relèvent du principe de droit suivant, tel qu'il se dégage de la dernière ordonnance de référé du Tribunal de Grande Instance de Paris prononcée à propos des propos homophobes tenus sur Twitter : ce sont les lois du pays dans lequel le service est offert qui priment, et non le lieu de stockage géographique des données. De même, dans le cadre d'un contrat français, le droit français s'applique.
Relativement au BYOD, il est nécessaire d'engager une réflexion sur une nouvelle définition de la vie privée, afin de pouvoir judiciariser les faits suspectés.
Afin d'améliorer la communication et la collaboration entre les différents services, des actions sont possibles : la SSI doit accompagner la DRH, l'aider à identifier les problèmes qu'elle n'a pas envisagés, l'alerter, afin d'éviter des interventions a posteriori, une fois le préjudice commis. Il faut également l'impliquer dans le dispositif de sécurité, l'embauche pouvant constituer un moment privilégié pour sensibiliser le nouveau salarié.

A12 - Smart cities : Quelle sécurité pour les villes de demain ?

Intervenants :

- Jean-François Janin : Chef de la mission « transports intelligents » ministère de l'écologie, du développement durable et de l'énergie,
- Benoit Kandel : Premier adjoint au maire, en charge de la sécurité, ville de Nice,
- Akim Oural : Conseiller communautaire pour Lille Métropole, en charge de l'économie numérique, ville de Lille.

Résumé des interventions :

Vidéo-protection intelligente, géolocalisation, Internet des objets... Ces technologies sont de plus en plus prisées dans l'optimisation des services de la ville de demain. Comment anticiper et gérer les vulnérabilités inhérentes à ces technologies et à leurs usages ?

I. Des villes de plus en plus intelligentes

Il n'existe pas, aujourd'hui, de ville intelligente « *smart city* » à proprement parler. Cela dit, l'introduction des TIC dans la ville ouvre la voie à de nouvelles fonctionnalités, de nouvelles manières de gérer, de gouverner et de vivre la ville qui façonneront les villes de demain. Ainsi de nombreux exemples existent en France de services urbains plus performants. Par le terme « *services urbains* » on désigne l'ensemble des services rendus par la collectivité sur son territoire pour les usagers, qu'il s'agisse des transports, de l'eau, de l'assainissement, des déchets, de l'énergie et des réseaux de télécommunication. L'utilisation des technologies de l'information et de la communication répond à deux objectifs principaux : optimiser la gestion des services urbains[1] et améliorer la qualité des services rendus aux usagers[2]. Pour ce faire, trois grands domaines sont concernés, les transports, les réseaux intelligents et la gestion technique centralisée.

1 - Lutter contre les émissions de Co2, économiser et mieux gérer l'énergie et les ressources décongestionner la ville, diversifier l'offre de transport, fluidifier les déplacements quotidiens, rendre plus performante la gestion municipale etc.

2 - Transport, accès aux services et équipements publics, sécurité etc..

- En ce qui concerne les transports, les objectifs sont nombreux : pour l'individu le but est d'améliorer les conditions de transport (du point de vue du confort, du temps d'attente, de l'accès aux informations), de bénéficier d'un meilleur accès aux transports et d'optimiser les déplacements. Pour la collectivité, cela permet de limiter la congestion urbaine et diminuer les émissions de CO2, de diversifier l'offre de transports, d'optimiser la chaîne de transports et offrir une meilleure information sur les modes de transports disponibles. Plusieurs solutions peuvent être mises en œuvre telles que : le guidage automatique pour trouver une place de parking, éviter la pollution ainsi que la

congestion liées à l'attente, la billetique qui offre un système d'interopérabilité entre les différents réseaux de transport, l'utilisation des ENR (véhicule électriques + bornes de recharges), la démultiplication de l'offre des modes de transport (plus particulièrement des transports publics individuels[3]), la gestion des déplacements par l'information multimodale, les routes intelligentes, la signalisation au sol, etc.

3 - Par exemple le vélib' et l'autolib'

- Pour les réseaux intelligents (eau, énergie…) il s'agit de faire face aux ressources limitées, au gaspillage, à la difficulté de gérer les pics de consommation, aux risques de coupures, aux zones de stress hydrique. Les objectifs sont pour l'individu, de réguler lui-même sa consommation grâce à une meilleure information sur sa consommation en temps réel, réduire la facture d'électricité, d'eau. Pour la collectivité, cela permet de préserver et économiser des ressources limitées, réguler offre et demande connaître les zones et les périodes de forte consommation.

- Les solutions sont variées : Smart grids : optimisation de la gestion de l'énergie par une meilleure régulation de l'offre et la demande et par l'intégration sur le réseau de distribution de la production locale d'énergies renouvelables. Cela comporte également une information en temps réel de la consommation d'énergie (grâce aux compteurs intelligents, comme Linky développé par ERDF), la construction d'îlots à énergie positive, la mise en œuvre de « *Smart water networks* » (capteurs et compteurs intelligents gérant les informations sur l'état du réseau, la consommation, les ressources disponibles, modèle de gestion dynamique en temps réel).

- Enfin, en ce qui concerne la gestion technique centralisée des services il s'agit de mettre fin au traitement des demandes par des services séparés, au manque de connexions entre les différents services et de fournir au citoyen une plus grande réactivité lors d'un dysfonctionnement. Pour une collectivité il s'agira d'optimiser le fonctionnement des services pour une économie des coûts de gestion, une efficacité accrue des services municipaux et une réponse rapide et efficace aux demandes des citoyens-usagers. Pour arriver à cela, différentes technologies peuvent être mises en œuvre : télégestion de l'éclairage public en fonction des conditions météorologiques, développement de systèmes automatisés (arrosage des espaces verts par exemple), création de bornes polyvalentes, comme la nouvelle génération d'horodateurs à Nice[4], etc.

4 -Ces horodateurs, grâce à un système d'information déployé via des « sensors » et des « meters » dans la chaussée, calculent instantanément le nombre de places disponibles et les dépassements horaires potentiels.

II. Anticiper et gérer les vulnérabilités

Si la ville intelligente présente un ensemble de solutions aux problèmes posés par le développement urbain et la gestion de la cité, il est nécessaire d'indiquer certaines limites induites par l'introduction des systèmes d'informations dans l'armature urbaine :

- Tout d'abord, nous pourrions assister à l'émergence de nouvelles formes d'exclusion liées à la non accessibilité aux TIC : exclusion des services publics numériques, exclusion sur critère économique, exclusion de la partie la plus âgée de la population, exclusion liée à des facteurs culturels, au niveau d'éducation… De même, on pourrait constater la prééminence d'une logique de l'offre sans prise en compte des besoins des usagers, de l'acceptabilité sociale et de l'appropriation de nouvelles

technologies. Mais aussi, on aurait à déplorer un coût très élevé pour les collectivités pour installer ces infrastructures numériques, avec risque d'inégalités croissantes entre les villes.

- Mais les deux principales limites concernent les vulnérabilités des systèmes d'information mis en œuvre pour réaliser toutes ces avancées technologiques. En effet les différents capteurs et compteurs surveillent de plus en plus l'action de chaque individu. Le traçage et le pistage, la rupture de la confidentialité, sont des dérives possibles. Nous le constatons de plus en plus, le piratage des systèmes centralisés de contrôle peut avoir des conséquences importantes voire graves. A titre d'exemple, il est possible de citer les différentes perturbations de circulation importantes dans certaines grandes villes des États-Unis suite au piratage du système de gestion des feux tricolores ou de certains réseaux ferrés. La deuxième vulnérabilité concerne la marchandisation de l'information. En effet, il est aisé de constater que, de nos jours, toute information peut présenter un intérêt certain et que celle-ci peut être détournée, volée, afin d'être revendue. Une maîtrise de la gestion et du contrôle de ces informations doit donc être une priorité au niveau de la sécurité et nécessiter la mise en place, non seulement de moyens technologiques, mais aussi et surtout une formation adaptée pour les personnels ayant accès aux différentes informations. On ne peut pas ignorer le risque de fuite d'informations sur l'architecture, les moyens de fonctionnement d'un système automatisé de gestion de l'eau par exemple, qui pourrait permettre une action terroriste. Le cyberterrorisme et la cyberguerre sont des phénomènes qui trouveraient un terrain propice de développement dans ce domaine précis des villes intelligentes.

- Dans le cadre de la ville intelligente, la sécurité à mettre en place s'appliquera non seulement à la sécurité physique des différents équipements mais également à la prise en compte de la sécurité des systèmes d'information, partie du dispositif vulnérable face à la montée en puissance de la cyber criminalité. Ce défi sécuritaire doit bien être pris en compte et surtout être une composante principale de toute étude visant la mise en place de technologie nouvelles dans le cadre du développement de la ville intelligente. Les atteintes aux systèmes SCADA, dont de nombreux exemples nous ont été donnés, doivent sensibiliser les décideurs de projets à la nécessité de maîtriser au mieux la sécurité des systèmes d'informations dans ce domaine

A13 - OTAN, UE ... Quelles alliances en matière de cybersécurité et de cyberdéfense ?

Intervenants :

- Olivier KEMPF
- Héli TIIRMAA KLAAR : cyber security advisor, Service Européen d'Action Extérieure.
- Patrice TROMPARENT (LCL) : Délégation aux affaires stratégiques (ministère de la dfense)
- Jamy SHEAH : Secrétaire général adjoint, OTAN.

Résumé des interventions :

Face au défi cyber, l'OTAN et l'UE cherchent à adapter leur organisation et à développer des capacités. Le périmètre des deux organisations pouvant se recouper et leurs moyens étant fournis par leurs membres (dont 21 sont communs), la question de la coopération se pose.

La volonté de coopérer, pourtant soutenue par la France, se résume dans les faits à un vœu pieux car les deux organisations sont en concurrence sur de nombreux points. Ainsi, les cadres de « *pooling and sharing* » (UE) et de « *Smart Defence* » (OTAN), destinés à conduire des projets multinationaux cherchent à drainer les financements. La crainte des Etats non membres des deux organisations d'être marginalisés freine également le rapprochement. Toutefois, les deux organisations, qui ont chacune leurs points forts et leurs points faibles, pourraient trouver avantage à coopérer pour partager les coûts, garantir l'interopérabilité et assurer une cyberdéfense totale de l'ensemble.

I. Etat des lieux

I.1 OTAN

Priorité explicite de l'OTAN depuis le sommet de Prague en 2002, la cyberdéfense dispose d'une politique ambitieuse et d'une organisation dédiée. Les cyberattaques en Estonie en 2007 et l'utilisation du cyber dans le cadre d'opérations conventionnelles en Géorgie (2008) ont renforcé cette détermination à intégrer pleinement la cyberdéfense dans le fonctionnement et les opérations. Il s'agit de donner à l'OTAN les moyens de poursuivre ses missions au profit de la sécurité collective des Alliés malgré les menaces pesant sur ses systèmes d'information et de communication. Cela inclut:

- la surveillance et la protection des réseaux

propres de l'OTAN (défense en profondeur) ;
- l'assistance éventuelle, sur leur demande, aux Alliés victimes d'une crise cyber majeure ;
- la coopération « à la carte » avec les partenaires, dont l'Union européenne, et l'industrie pour mieux appréhender les menaces et les solutions.

Le NCIRC (NATO Computer Incident Response Capability) a été créé pour assurer la supervision des réseaux de l'OTAN et la réaction face aux attaques. Il dispose d'équipes de réaction rapide prêtes à intervenir sur les réseaux de l'OTAN ou à assister des Alliés qui en exprimeraient le besoin. Un centre d'expertise pour la cyberdéfense a été créé par l'Estonie et s'est vu attribuer le statut de centre d'excellence de l'OTAN. Suite au sommet de Chicago de 2012, des projets cyber sont possibles dans le cadre de la Smart Defense qui vise à permettre aux Alliés de développer ensemble des capacités militaires. Seul un projet est pour l'instant proposé. Des questions importantes restent posées: activation de l'article 5 en cas d'attaque cyber, périmètre de l'assistance de l'OTAN sur les systèmes des Alliés (OTAN et/ou nationaux? Militaires et/ou civils?).

II.2 Union Européenne

Initialement considéré sous l'angle de la protection des infrastructures civiles critiques et comme support des valeurs de l'UE (liberté d'expression, démocratie, protection de la vie privée) et du développement économique, le cyber a tardé à faire l'objet d'une stratégie globale. Cette stratégie parue en février 2013, a un objectif global:
- investir dans ce secteur industriel et augmenter la cyber-résilience des infrastructures critiques,
- réduire la cyber-criminalité (création au 1er janvier 2013 d'un centre européen de lutte contre la cybercriminalité, soutien à la convention de Budapest),
- Inclure un volet cyber dans la PSDC et promouvoir la coopération avec l'OTAN.

L'UE dispose d'un centre de veille et de réponse pour ses réseaux (CERT-UE) et d'une Agence pour la Sécurité des Systèmes d'information (ENISA) qui développe une expertise. Sur le plan capacitaire, l'Agence Européenne de Défense, qui conduit les projets communs des Etats-membres, a inscrit le cyber comme une priorité, tandis que le cadre multinational du Polling and Sharing peut accueillir des capacités cyber.

II. La coopération

L'OTAN est une alliance militaire pragmatique qui considère que des défaillances des systèmes critiques civils obéreraient ses capacités opérationnelles. Pourtant, son assistance liée à une mise en œuvre de l'article 5 devrait se limiter aux cas d'agression armée, ce qui n'est pas toujours évident en cyber. A contrario, l'UE est une organisation globale dont le traité prévoit non seulement une clause d'assistance en cas d'agression armée de l'un de ses membres (art 42.7 du Traité de l'Union Européenne) mais aussi une clause de solidarité en cas d'attaque terroriste ou de catastrophe industrielle ou d'origine humaine (article 222 du Traité sur le fonctionnement de l'UE). De plus, l'UE a des compétences dans de nombreux domaines civils liés au cyber (communications, commerce, économie, R&D, etc.). Son champ d'intervention serait donc plus large que celui de l'OTAN.
Une coopération semble donc inévitable pour éviter de dupliquer les moyens (et éviter les dépenses inutiles aux 21 membres en communs) notamment en matière de défense. Mais d'une

façon générale, l'OTAN et l'UE coopèrent mal: influence des Etats hors UE (Etats-Unis et Turquie), enjeux industriels nationaux, partage des tâches de fait, quoique notamment contestée par la France (organisation militaire OTAN éprouvée, soft power de l'UE), préférence pour l'OTAN des petits pays de l'UE (réassurance en dernier ressort avec les Etats-Unis). De plus, les Nations ne partagent en cyber qu'avec réticence car c'est un domaine sensible pour la souveraineté nationale et très confidentiel. Les coopérations internationales se limitent à de petits cercles de confiance pour les aspects les plus opérationnels, même si de grandes enceintes (ONU, IUT, OSCE, AIEA, ...) peuvent accueillir des débats très généraux.

Conclusion

Si l'OTAN et l'UE sont toutes deux légitimes dans leurs attributions, le continuum sécurité défense du cyber brouille la répartition des rôles. Chaque organisation, poussée par sa logique interne, tente d'étendre son périmètre. L'UE qui est plus globale aurait l'avantage si elle prenait mieux en compte les aspects militaires de la cyber, face à un OTAN plus efficace et plus attractif pour les petits pays. La coopération va de toutes façons devoir se mettre en place, si ce n'est pour établir des réglementations et des normes compatibles entre les Européens et les Américains, au moins pour assurer une gestion de crise efficace en cas d'incidents cyber qui pourraient avoir de graves conséquences sur le territoire européen.

A14 - Existe-t-il un marché pour la cybersécurité ?

Intervenants :

- Eric Domage : directeur de la stratégie, BU sécurité, Orange Business Services,
- Mathieu Poujoul : Principal consultant, Cloud, Security & Middleware, Pierre Audoin Consultants,
- Jean-Pierre Quémard : président de l' Alliance pour la Confiance Numérique (ACN),
- Thierry Rouquet : Président directeur général (Arkoon),
- Sébastien Héon : Directeur des affaires publiques (Cassidian CyberSecurity),

Résumé des interventions :

Le marché de la cybersécurité existe et se développe très rapidement. Il doit toutefois être mieux structuré, tant du côté de l'offre que de celui de la demande. Une politique industrielle s'appuyant sur la R&D et la création de consortiums conditionnent la consolidation d'un secteur qui bénéficie en France d'un potentiel technologique reconnu mais encore trop dispersé.

Le marché de la cybersécurité affiche une croissance de 10% par an et un chiffre d'affaires de cinq milliards d'euros (et autant à l'export), selon une étude réalisée (2013) par l'Alliance pour la Confiance Numérique. En France, environ 600 « *start-up* » emploient près de 50.000 personnes. Ce développement rapide du marché de la cybersécurité s'observe aussi dans d'autres pays qui exercent aujourd'hui un véritable « *leadership* », les Etats-Unis en particulier. Observe-t-on un phénomène passager, la création d'une « *bulle* », ou bien l'émergence d'un marché durable en expansion constante?

I. Un marché en devenir

La question posée appelle une réponse unanime des participants. Il existe un marché pour la cybersécurité mais celui-ci est encore jeune et pas complètement structuré. Cela se vérifie tant pour l'offre que la demande :

- du côté de l'offre, les outils proposés sont souvent très innovants, mais ils ne sont pas toujours suffisamment intégrés pour répondre globalement aux problèmes des clients. Il faut que l'offre se structure en des solutions plus transverses. De plus, sous le même vocabulaire (Security Information and Event Management- SIEM ou System on a chip- SOC, etc.) on retrouve des produits de qualité très variable, ce qui complique la structuration de la demande.
- du côté de la demande, en effet, les clients n'ont pas tous la capacité de faire la différence entre des solutions haut de gamme et des offres standardisées. Il en résulte un nivellement par le bas des offres et des prix qui ralentit le

développement du marché de la cybersécurité.

II. Une structuration des acteurs qui fait débat

La structuration des prestataires de solutions de cybersécurité a fait débat : comment garantir l'innovation nécessaire quand le tissu industriel est très morcelé, quand les entreprises disposent de budgets de R&D très faibles comparés notamment à ceux des « *géants américains* »? Dans ce contexte peu favorable, l'organisation de la politique industrielle repose sur deux conditions essentielles.

La première porte sur l'obtention de financements publics pour stimuler la R&D. Ces financements peuvent être européens, via les projets qui relèvent du Septième programme-cadre (FP7), actuel programme (2007-2013) géré par la Commission de l'Union européenne pour développer la recherche et le développement technologique. Les financements peuvent aussi être nationaux, via les Investissements d'Avenir pour développer la recherche et soutenir les filières d'excellence, les « *programmes d'études amont* » de la Direction générale de l'Armement (DGA), etc. Ces mécanismes ont l'inconvénient d'être complexes, notamment lorsqu'ils doivent être mis en œuvre par des PME. S'agissant des suites, que reste-t-il concrètement d'une étude papier financée par Bruxelles ?

La deuxième condition porte sur la création de consortiums au niveau européen regroupant des PME et de grandes entreprises. L'objectif est de renforcer à la fois la capacité d'innovation des grands groupes en s'appuyant sur des PME très agiles et innovantes, et de faciliter l'accès aux marchés export que les petites structures ne peuvent pas démarcher seules.

Il se dégage de cette table ronde un consensus sur la nécessité de structurer tant le marché que le tissu industriel de la cybersécurité. Cette stratégie n'est pas une utopie, car les entreprises françaises offre un très fort potentiel technologique et une performance reconnue sur les marchés internationaux (exemples d'Arkoon et de Cassidian).

A15 - de l'activisme à l'hacktivisme

Intervenants :

- Damien BANCAL : Zataz,
- Nicolas DANET : co-auteur de Anonymous, pirates informatiques ou altermondialistes et consultatn au sein de l'Agence Limite,
- Nicolas DIAZ : responsable des systèmes d'information pour la FIDH / Hacktiviste,
- Jean-Marc BOURGUIGNON : Hacktiviste, conseiller en sécurité et confidentialité de l'information, collectif Telecomix,
- Cécile DOUTRIAUX : avocate au barreau de Strasbourg.

Résumé des interventions :

Le phénomène hacktiviste occupe une place grandissante dans l'actualité grâce à la médiatisation dont bénéficient certains collectifs comme Anonymous. Insaisissable par nature et évoluant en permanence, il désigne les activités de collectifs aux profils et modes opératoires très variés (du défacement de site au rétablissement de connexion Internet dans des pays faisant l'objet de censure). Cette nouvelle forme de contestation politique exploitant de façon transgressive l'outil informatique coexiste avec d'autres formes de contestation plus classiques.

I. Etat des lieux

Dans les années 1990, à la naissance du web, l'activiste était un militant considéré comme extrémiste. Pour faire entendre sa cause, il utilisait la propagande, le lobbying, la désobéissance civile et les opérations coup de poing. Avec la modernisation de la société, nombre d'activistes ont changé de modus operandi pour devenir hacktivistes. Le terme « *hacktiviste* » est d'origine angloaméricaine.Il est dérivé du mot « hacker ». Il s'agit d'un individu qui essaie de comprendre le fonctionnement d'un mécanisme pour ensuite le détourner de sa vocation originelle. L'hacktivisme renvoie donc à un mouvement de personnes qui s'emparent de la technologie accessible à tous, en l'espèce d'internet, pour militer et véhiculer des messages. « Anonymous » est un exemple de groupes se revendiquant comme « *hacktiviste* » et utilisant la toile pour faire passer des messages par des actions médiatiques. De caractère international, il ne présente cependant aucune structure officielle et semble totalement désorganisé. En effet, les agissements de certains membres ne sont pas cautionnés par d'autres.

« *Anonymous* » n'est pas le seul groupe hacktiviste présent sur internet. Il semble pourtant prendre une part médiatique importante, empêchant certains d'atteindre la notoriété nécessaire à

la publicité de leurs actions. Par exemple, en 1996, a eu lieu le plus grand rassemblement altermondialiste à Seattle. Un groupe du nom d'Electrohippie a réalisé des attaques par déni de service sur l'OMC. Ces attaques qui sont habituellement utilisées par les Anonymous n'ont eu qu'une répercussion médiatique faible. Récemment, en Tunisie, le groupe « *Takriz* » avait défié la censure tunisienne sous le régime du président Ben Ali.

II. Les divergences et oppositions éventuelles

Au même titre que les opérations coup de poing, on pourrait considérer que les attaques par déni de service, modus operandi utilisé par le groupe Anonymous, n'entrent pas dans le champs de l'art hacktiviste. Pourtant Anonymous revendique être un groupe hacktiviste, alors que pour certains il n'est qu'un groupe activiste parmi tant d'autres. Anonymous devient alors une sorte d'agence de communication de l'activisme sur internet. L'hacktivisme et son impact sur l'activité économique ou sur la réputation d'une entreprise ou d'une institution, engendrent une médiatisation de la cause défendue. Les hacktivistes visent ainsi à mobiliser l'opinion et à obtenir le soutien des citoyens.
Sur le plan légal, les hacktivistes entretiennent ce qui leur semble juste en équité et non pas en règle de droit. Ils se réfèrent à deux textes fondateurs : le « *manifeste du hacker* » et « *la déclaration d'indépendance du cyberespace* » en 1996. Les hackers considèrent que leurs règles dépassent les frontières. En ce sens, ils établissent leur propre rèférentiel. La barrière de la légalité semble être maintenant continuellement franchie par les hacktivistes. La divulgation sur les réseaux sociaux de l'identité de certains agresseurs présumés du viol d'une femme en sont une illustration. Cependant, une considération objective du phénomène démontre que les groupes tant activistes qu'hacktivistes n'ont aucune reconnaissance légale et qu'ils ne sont composés que de personnes autoproclamées qui ne représentent qu'une part minime des sociétés modernes.

III. Les attentes qui émergent des débats

D'une manière générale, la crédibilité du mouvement hacktiviste va évoluer de manière positive selon les termes d'une certaine régulation interne. Il est un fait que certaines actions décrédibilisent des groupes entiers au gré de dérives plusieurs fois constatées. On peut estimer que de nouveaux groupes plus locaux devraient voir le jour, au détriment de la bannière Anonymous dont certains membres sont devenus pratiquement incontrôlables. L'hacktivisme apparaît également comme une nouvelle forme d'expression politique qui, dans sa dimension virtuelle, a de réels impacts. Son avenir incertain pourrait s'inscrire dans un partenariat avec le monde associatif. Il peut susciter une transmutation en hackers politiques, à l'instar du soutien des Anonymous au mouvement Occupy ou encore de la participation de certains agents Telecomix à la mobilisation contre le projet de construction d'un aéroport, à Notre-Dame-des-Landes. Plus encore, réalité et cyberespace s'influent mutuellement jusqu'à faire émerger des formes inédites de participation politique, le Parti Pirate, en alliant représentation conventionnelle et idéologie issue principalement de la culture hacker.

A16 - Quel parcours pour les particuliers et les entreprises victimes d'actes criminels ?

Intervenants :

- Maitre Corinne CHAMPAGNER-KATZ : avocat (cabinet CCK),
- Patrick LANGRAND : RSSI groupe, groupe La POSTE,
- Sylvain THOMAZON : huissier de justice associé, SCP LACHKAR, GOUGUET, THOMAZON, BICHE,
- Jean-François MASSELIS : Directeur du service intercommunal d'aide aux victimes de la ville de Roubaix,
- Éric CAPRIOLI : Avocat à la cour, Paris.

Résumé des interventions :

Les difficultés spécifiques de la lutte contre la cyberdélinquance conduisent à recommander une démarche rationnelle et le recours à une expertise.
Les enjeux sont dès lors relatifs à une définition normative des actes à opérer, à une politique d'alerte et d'information et de sensibilisation générale des acteurs. Ils soulignent la primauté du constat d'huissier et du recours aux spécialistes NTECH de la police et de la gendarmerie nationale.

I. Le consensus

La prise en compte des actes dont peuvent être victimes les particuliers et surtout les entreprises renvoie naturellement au rôle de l'huissier de justice et à la force probante de son « *exploit* ».
Le constat d'huissier peut ainsi intervenir à tout moment. Sa force probante en fait le point de départ de toute prescription légale. Le constat sur requête permet l'intervention chez un tiers, garantissant la copie des disques durs au même titre que la « saisie-contrefaçon », les injonctions de communiquer s'agissant des adresses IP, etc. S'agissant d'infractions pénales, au travers du recours aux services de police et de gendarmerie nationale, l'appel aux spécialistes NTECH[1] est gage d'efficacité et garant de la rapidité de l'intervention. Il faut néanmoins reconnaitre une difficulté : la réticence de certaines victimes à déposer plainte par peur pour leur réputation, mais aussi compte-tenu de la difficulté à évaluer le préjudice.

1 - Gendarmes et policiers, habilités sur le plan judiciaire, détenant du fait d'une formation spécifique les capacités à instrumenter en mobilisant toutes les technologies propres à la manifestation de la vérité (Traces biologiques, traitement de l'image, du son, exploration des surfaces de disque, investigations sur les réseaux, etc...)

II. Les attentes

Les victimes attendent une aide dans leur cheminement. Les difficultés résident dans le caractère transnational des bandes organisées, la nationalité des sites, rarement français, l'identification des auteurs et le risque d'atteinte au secret des affaires. Se surajoutent à ces paramètres des problèmes matériels : choix de la trace qui doit être détectée ou identifiée, validation des cibles qu'il convient de privilégier en protection, les modalités d'anticipation afin d'organiser une réaction efficace.
L'aide aux victimes (environ 500 000 par an) s'inscrit dans la durée. Dans ce domaine, on procède à une classification en deux entités : le groupe « arnaques » et le groupe intitulé « cyberintimidation ». Enfin, pour mieux aider et prévenir les victimes présentes et futures, il s'agira de les informer sur le rôle et le potentiel de la « *CIVI* »[2] notamment quant au régime des indemnisations pour réparation du préjudice.
Le groupe « *La Poste* » a, pour sa part, résolu de faire appel aux experts du droit et de l'analyse de risque. Son directeur RSSI met par ailleurs en exergue le lien obligatoire entre les deux fonctions majeures de RSSI et de directeur de la sécurité. Par ailleurs, la problématique de la contrefaçon et la spoliation des sites marchands ont également justifié la démarche de jeter des « *ponts* » complémentaires entre ces deux fonctions. L'infrastructure managériale et informatique de la Poste, vitale pour le fonctionnement de la Nation, prend en charge une vaste palette de fonctionnalités. Outre les métiers de la Banque, elle embrasse la protection du courrier, des colis et la gestion voire l'interaction de 17000 points de contact avec les clients.

2 - Commission d'Indemnisation des Victimes d'Infractions. La CIVI est composée de deux magistrats et d'une personne qualifiée pour les problèmes de victimes. http://www.association-aide-victimes.fr/

En conséquence, en matière de disponibilité des systèmes d'information, une interruption de service peut générer une crise. Une « *cellule de crise* » pro-active a été créée afin de coordonner, d'organiser une réponse immédiate aux dysfonctionnements revêtant une gravité et nécessitant la gestion de opérateurs ayant une expertise différentes mais nécessaire à la résolution de la crise. Ses moyens reposent totalement sur ceux de la SSI.

III. Les enjeux

Les enjeux engerbent désormais le droit de l'information et atteignent les frontières de la contrefaçon, dont la gravité est désormais reconnue.
Les types d'infractions recensées sont essentiellement des escroqueries, des ventes sans livraison, des atteintes à l'image, des incitations à la haine raciale, des diffamations...

Démultipliées par l'ampleur du cyberespace, les mesures de riposte à adopter sont en croissance exponentielle permanente.
Elles reposent sur :
- la nécessité de figer l'instant dans les vols d'informations et l'usurpation d'identité,
- le référencement des tentatives d'intrusion,
- le calibrage des procédures de sécurité à respecter et l'identification des traces à conserver.

Il convient par ailleurs de :
- réaliser une charte des utilisateurs,
- définir une politique d'alerte générale et communiquer sur les objets.

A17 - Cybersécurité : quels enjeux pour les SCADAS énergétiques ?

Intervenants :

- Nicolas Mazzucchi : Polemos Consulting,
- Gérard Pesch : chef du secteur conseil en sécurité et évaluation – Thales,
- Edouard Jeanson : vice- président, directeur technique de l'activité sécurité – groupe SOGETI,
- Jean-Pierre Hauet : président – ISA France,
- Christophe Renard – consultant, HSC.

Résumé des interventions :

Si les SCADA sont indispensables à la bonne administration de la distribution des énergies par les groupes fournisseurs, il convient de les approcher en terme de sécurité globale. En effet, la plupart des grandes entreprises de production en sont tributaires. Le risque inhérent aux interconnexions et à la multiplicité des acteurs ayant accès aux SCADA dans les entreprises étant bien réel, le secteur de l'énergie revêt un caractère particulier, car non seulement les implications sont économiques, mais elles ont aussi un lourd impact stratégique. Une expertise naissant dans ce domaine permet de dégager des axes de réflexions qui pourraient accroître la sécurité des SCADA[1] tant en travaillant sur les domaines de la technique ou de la normalisation qu'en travaillant sur l'éducation des acteurs.

1 - Un SCADA, acronyme de l'anglais Supervisory Control And Data Acquisition (télésurveillance et acquisition de données), est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques.

Un SCADA est un système de télésurveillance et de gestion d'installations techniques qui ne s'applique pas qu'au domaine énergétique. Les SCADA sont nés à partir des années 60 dans le secteur industriel. Les grands groupes de fourniture d'énergies, dont l'exploitation est très étendue du fait du maillage des réseaux de distribution, y ont très rapidement vu leur intérêt. En effet, la supervision pouvait être centralisée et on pouvait avoir un regard direct sur le bon déroulement du processus. Avec cette avancée est née une certaine perméabilité entre les réseaux de travail qui s'est rapidement muée en vulnérabilité.

I. Le risque lié à l'intégration de la cybersécurité dans le processus industriel

L'objectif managérial de celui qui met en œuvre un SCADA est l'optimisation de la production. Dans le domaine énergétique, il s'agira d'optimiser la consommation en diminuant les

pertes sur le réseau. Dans ce terme, l'enjeu de l'intégration des SCADAS énergétiques au monde Cyber pose la question de la relation privilégiée entre l'énergéticien et le spécialiste en cybersécurité.
Au départ, les entreprises spécialisées proposaient des prestations en matière de sécurité informatique dite classique. A la demande des clients, elles ont commencé à travailler sur la sécurisation des SCADA. Cette demande a fait suite à l'apparition du ver conficker. Pour se prémunir de ce genre d'attaque, les entreprises ont voulu isoler les réseaux contrôlant leurs chaînes de production des autres réseaux de travail. Cette vulnérabilité était nouvelle et nul n'avait auparavant pensé que les réseaux d'exploitation de chaînes de productions pourraient être la cible d'attaque. Il a donc fallu sensibiliser les industriels aux risques engendrés par la connexion de ces réseaux au monde IP.
Appliqué aux SCADA énergétiques, ce risque prend une toute autre dimension lorsqu'on imagine l'impact qu'aurait une cyberattaque paralysant le réseau de distribution d'eau ou d'électricité d'une grande ville. Le domaine énergétique est très particulier au sein du secteur industriel, car il comprend une dimension fortement stratégique.
Le risque pesant sur les SCADA énergétiques comporte deux aspects essentiels : l'espionnage ou encore le sabotage qui est le risque majeur. En effet, le déni de service est totalement paralysant pour une entreprise car l'évolution de l'informatique industrielle a supprimé le cloisonnement qui existait auparavant entre les trois niveaux que sont la gestion de production, la gestion interne de l'entreprise et la gestion de l'ensemble de ses cellules. Le monde industriel connait une vraie difficulté à s'adapter à ces nouvelles menaces. Dans ce secteur, la prévention s'exerce beaucoup plus contre l'accident que contre l'atteinte délibérée.
Une autre différence de culture est à soulever : dans le domaine industriel, le cycle de vie d'un système de type chaîne de production est estimé à une trentaine d'année. Or, l'informatique d'entreprise connait un cycle de vie qui ne dépasse pas 5 ans et qui subit durant ces cinq années, bon nombre de modifications et de mises à jour.

II. Une protection possible grâce à l'anticipation et la formation

La prise de conscience est très récente. En août 2012, le groupe pétrolier saoudien ARAMCO a vu 40.000 de ses ordinateurs infectés par un virus introduit par un employé dans son réseau informatique. Des cas similaires ne connaissent qu'une publicité restreinte car leur révélation par une entreprise victime d'une telle attaque donne une image extrêmement négative.
La solution s'articule en deux axes que sont la formation et la réactivité. La question de la formation intéresse le champ universitaire mais également l'éducation des acteurs de l'entreprise à tous les niveaux. Il faut ensuite actualiser cette formation auprès des décideurs et des managers pour qu'elle soit diffusée le plus largement possible au sein des différentes strates de l'entreprise. Quant à la réactivité, il convient d'instaurer des procédures de « réactions » et de désigner des responsables de l'application de ces procédures. L'acquisition de bons réflexes et la capacité de les mettre en œuvre rapidement se travaille et se teste lors d'exercices de simulation. Par exemple, la Banque de France pratique des tests de réactivité dans le cas d'une cyberattaque.
La composante normative pour se prémunir des risques s'est appuyée sur la norme ISA 99[2] qui

a initié un processus de standardisation. Elle a pour double objectif de poser les bases d'un cadre méthodologique permettant de bâtir la cybersécurité d'une entreprise et de créer un niveau de confiance en un système donné. L'approche normative repose sur deux idées majeures . Il s'agira d'abord de transposer dans le domaine Cyber ce qui fonctionne dans le domaine de la sécurité fonctionnelle : l'analyse du risque associée à l'état des lieux des mesures en place mettra en lumière un niveau de confiance à accorder au système. La deuxième phase consacrera l'application du principe de la défense en profondeur.

De manière générale, la durée de vie d'un système industriel est trop longue pour faire l'objet d'une intégration de cybersécurité. Il s'agit alors avant tout de définir des règles comportementales à inculquer et entretenir auprès des différents acteurs qui travaillent avec les SCADAS en tenant compte de ce différentiel et de l'intégration progressive de structures logicielles sur un ensemble hétérogène.

En choisissant de vivre dans un environnement informatique permanent, comme le souligne le développement du Cloud, il faut accepter un risque permanent. Par analogie, la vie implique l'acceptation du risque de la maladie mais la crise survient si tout le monde est malade en même temps. La gestion du risque sanitaire vise à éviter cette atteinte simultanée et dans le pire des cas l'extinction d'une ecosphère. Il en va de même dans le domaine informatique.

2 - Les travaux de normalisation les plus avancés ont été menés aux US depuis le début de la décennie. Les travaux du comité ISA SP99 ont bénéficié de l'effort de recherche US et des travaux de normalisation sectorielle (Scada,Chimie,Energie ...) et ont conduit à la publication d'un certain nombre de documents de base : rapports techniques et standard ISA / ANSI. Un rapprochement a été effectué récemment en vue de rédaction commune avec le comité 65 de la CEI (le standard IEC 62443 reprenant tous les standards ISA 99 existants).

A 18 - Les APTs (Advanced Persistent Threat) : vraie menace ou coup marketing ?

Intervenants :

- Nicolas RUFF : chercheur en sécurité informatique (EADS),
- David BIZEUL : expert en sécurité informatique (Cassidian CyberSecurity),
- Michel DUBOIS : ingénieur en sécurité informatique (France.securipros),
- Yves LE FLOCH : directeur du développement de la cybersécurité (SOGETI),
- Yogi CHANDIRAMANI : directeur technique Europe (FireEye).

Résumé des interventions :

La notion d'APT (Advanced Persistent Threat) désigne des cyberattaques ciblées très complexes. Qualifiées par certains observateurs de « scénarios catastrophe » relevant du marketing, ces attaques réelles relèvent de stratégies techniques, d'analyse de cibles et de vulnérabilités des systèmes hôtes. Elles débouchent sur une appropriation des données sensibles d'une entreprise via la conquête des droits d'administration d'un utilisateur et la mise en place d'un mécanisme masqué visant à créer un univers fictif pour la cible. Les protections contre ce type d'attaque résident dans l'application des règles élémentaires de sécurité et une organisation en profondeur de la défense du système.

I. Les problématiques

Ces attaques résident dans la mise en place d'un serveur de commande et de contrôle. Le site internet de la victime va être pollué par l'installation d'un programme visant à inviter les victimes à utiliser un site. Une fois ces sollicitations mises en œuvre, l'objectif est de compromettre au moins un ordinateur faisant partie d'un réseau d'une entreprise ou d'une administration. L'idéal étant de pénétrer la machine d'un utilisateur possédant le maximum de droits d'administration. Ce « tunnel » sera utilisé pour récupérer un maximum d'informations ou compromettre voire détruire des données. La description des attaques de type APT qui ont affecté diverses cibles, tant des administrations que des entreprises, permettent d'établir que les techniques utilisées ne sont pas de premier ordre. Il s'agit souvent d'un mailing comportant des pièces jointes porteuses du programme parasite qui invitent à une réponse et une interaction avec d'autres acteurs de l'entreprise assurant une propagation interne du *malware*. Le degré de sophistication réside plutôt dans la capacité à isoler et saisir l'environnement socio-professionnel de la cible et son appareillage informatique (les noms de certaines personnes,

les processus de l'entreprise et les moyens techniques, etc...). Il est complété par le soin apporté à la préparation et à la conception du logiciel malveillant. C'est une attaque en profondeur qui vise pour les plus aboutis au contrôle total du système d'information et à la modification des processus de l'entreprise. La difficulté pour les programmes assaillants étant d'émettre des signaux faibles, discontinus dans le temps et n'affectant que quelques cibles pour ne pas éveiller l'attention du RSSI.
Ces attaques sont mises en œuvre par des acteurs aux profils différents sans occulter une dimension étatique. Le développement et la mise en œuvre du virus « stuxnet » visant les centrales nucléaires iraniennes exigent un haut niveau de technicité que seul un Etat peut maîtriser. Les associations de crime organisé ont très vite saisi l'intérêt de ce type d'attaque afin de pouvoir toucher un maximum de victimes tout comme les cybercriminels plus solitaires. Enfin, les groupes d'hacktivistes ont aussi saisi cette opportunité dans une vocation politique ou pour porter et de faire connaître des revendications au travers le signal fort d'une destruction d'une infrastructure informatique.

II. Des solutions

Les dispostifs habituels : firewalls, les antivirus ou les IDS[1] ou IPS[2] n'offrent pas de garanties quant à ce type d'attaques. Les concepteurs de programmes malveillants se garderont d'utiliser des outils dont les signatures sont connues des antivirus.

1 - IDS (Intrusion Detection System) : mécanisme destiné à repérer des activités anormales ou suspectes sur un réseau ou un hôte.
2 - IPS (Intrusion Prevention System) est un outil permettant de diminuer les impacts d'une attaque, de détecter un balayage automatisé d'un site. Il permet de bloquer automatiquement des ports d'accès mais n'a pas toujours la sélectivité attendue.

Les mesures de sécurité passent par l'application des règles élémentaires de sécurité informatique, les attaques se diffusant principalement par les pièces jointes contenues dans les emails. Il faut donc mettre en place des outils de sécurité spécifique visant à déceler la compromission. L'officier de sécurité, sensé connaître les failles de son système et ses vulnérabilités, devra positionner des sondes. Il pourra organiser le contrôle de fichiers bureautiques provenant des messageries (vérification des objets exécutables, URL[3] suspectes, routages automatiques de réponses, ...). La surveillance du download de fichiers depuis l'Internet, l'examen des alertes des antivirus de type heuristique, la surveillance d'accès aux clés de registre susceptibles d'exécuter des programmes sont la base d'une salubrité du système d'entreprise.

3 - URL (Uniform Resource Locator), grossièrement une adresse Web, désigne une chaîne de caractères pour adresser les ressources du www : document HTML, image, son, forum, BAL, etc...

En conséquence et globalement, il faut développer une bonne hygiène informatique : isoler les postes et les ordinateurs à risque au sein d'une entreprise. Une bonne administration permet d'éviter qu'une éventuelle contamination ne se diffuse à l'ensemble du réseau. De plus, les APT étant difficiles à parer, il faut développer une défense en profondeur au travers d'une élévation des niveaux de protection dans les entreprises.
Enfin et en conclusion, il apparaît opportun de développer une politique de gouvernance de cybersécurité et des outils de prospective afin d'anticiper les conséquences d'une éventuelle attaque. Cela passe éventuellement par une décentralisation des réseaux afin de diminuer les risques. Le développement de la «résilience» au sein des entreprises et des administrations est, dès lors, un objectif fondamental.

A 19 - Dématérialisation et archivage

Intervenants :

- Thierry PIETTE-COUDOL : Avocat, TPC Avocats,
- Jean-Louis BAJU : Directeur du Centre de gestion de la fonction publique territoriale,
- Alexandre BARBOT : Responsable commercial sécurité intérieure, Sopra Group,
- Emmanuel MICHAUD : Directeur délégué Chronoservices, Imprimerie nationale,
- Jean-Marc RIETSCH : Président, FEDISA.

Résumé des interventions :

L'écrit électronique a la même valeur que le support papier au regard de la loi. La question de sa conservation est donc stratégique pour les collectivités et les entreprises. Le passage à la dématérialisation nécessite un questionnement du client et une organisation sécurisée quant au format de la donnée, au mode de stockage, un accès privilégié et à une migration itérative afin d'accompagner l'évolution des standards et formats de fichiers.

I. Les idées fortes

Il ne faut pas confondre dématérialisation et gestion électronique de documents (GED). Le terme « *dématérialisation* » recouvre plusieurs opérations : la numérisation des documents proprement dite, à laquelle on l'assimile le plus souvent, mais également l'organisation des échanges de documents numérisés et des processus « *métiers* » qui en découlent. La question de la dématérialisation relève donc autant du domaine juridique et technique que du domaine organisationnel.

A l'origine, l'archivage électronique relevait des directions informatiques qui traitaient la question essentiellement sous l'angle technique. Or, la technique ne prend pas en compte toutes les problématiques de la dématérialisation, notamment celles qui relèvent de l'archivage proprement dit. Depuis peu, la collaboration entre informaticiens et archivistes est revenue au cœur des processus de dématérialisation. On se rend compte que l'archivage électronique fait partie intégrante du système d'information de l'entreprise.

La conservation de documents dématérialisés (ou archivage électronique) a pour objectif de permettre à l'utilisateur de retrouver une information dont l'origine et l'intégrité doivent être garanties. L'archivage ne concerne que des documents définitifs qui ne sont plus appelés à évoluer et qui doivent être conservés sur le long terme. L'important est donc la sécurisation de l'information dans le temps. Plusieurs solutions existent. Les entreprises peuvent utiliser des « armoires numériques » qui équivalent à une sorte de coffre fort électronique. Ce qui confirme la proximité croissante entre dématérialisation et

archivage. Certaines font appel à des stockages externes (informatique en nuage ou e-Cloud) avec les problèmes de sécurité que l'on connaît. Depuis peu l'État met à disposition des particuliers des espaces de stockage sécurisés sur /www.service-public.fr/. Des réflexions sont d'ailleurs en cours concernant le stockage et la réutilisation de documents ou de données stockées par les utilisateurs afin de faciliter leur démarches administratives.
La sécurité a un coût mais elle est majeure car elle est à la base de la confiance accordée aux documents numériques. Elle conditionne aussi les plans de continuité d'activité et les plans de reprise d'activité. Les paramètres techniques de sécurité existent de la signature électronique à l'horodatage des serveurs. L'ANSSI a établi une liste de produits certifiés et la DISIC1 donne également des règles à adopter. Les nouvelles technologies font que l'on évolue peu à peu de la gestion de la sécurité à la gestion des risques.
Au-delà des nombreuses règles pour sécuriser l'archivage, il convient de se conformer aux lois concernant la conservation des donnés à caractère personnel et d'obtenir l'accord indispensable de la CNIL. Les données à caractère personnel peuvent être conservées 3 à 5 ans. Au-delà, elles doivent être obligatoirement anonymisées. Les directives européennes sont très protectrices en matière de données personnelles mais des discussions sont en cours pour autoriser la conservation à plus long terme.
La restitution des données peut poser des problèmes techniques. En fait, le support n'est plus vraiment un obstacle, c'est plutôt l'interprétation qui peut s'avérer difficile voire impossible dans le temps à cause de l'évolution des technologies, des changements de formats, etc. Pour l'heure, il n'y a pas de solution. Il faut seulement anticiper la conversion de format en organisant des migrations régulières et en suivant de près les évolutions matérielles et logicielles. Certaines sociétés organisent ces migrations pour leurs clients à intervalles réguliers afin de préserver l'intégrité des données archivées. Cela représente un coût qui peut rendre l'archivage électronique plus onéreux que l'archivage papier. A cet égard, il est d'ailleurs important de préciser que la mise en place d'un processus de dématérialisation représente un investissement important surtout lorsque il y a plusieurs unités. Il faut une véritable volonté politique et des moyens pour le mener à terme.

II. Les conditions d'une dématérialisation réussie

Un accompagnement est indispensable. Tout d'abord, il faut impliquer le client très en amont pour définir ses besoins précisément et mettre en place des processus et des infrastructures adéquates. Cependant, les solutions techniques impactent peu sur le succès. En revanche, la pédagogie est indispensable pour faire accepter de nouvelles habitudes de travail.
La dématérialisation induit en effet des changements importants dans les habitudes de travail et les réticences sont parfois nombreuses. Par exemple, la signature électronique qui permet de sécuriser le système est souvent difficile à faire accepter notamment par les cadres dirigeants. Toutefois, l'expérience prouve que lorsque l'on décide de conduire des projets de dématérialisation, il faut éviter de faire coexister papier et support électronique car cela entraîne inévitablement un système à deux vitesses et, à terme, l'échec du processus de dématérialisation.

A20 - Technologies de l'information et de la communication et ordre public

Intervenants :

- Denis FORTIER : Directeur de la rédaction d'AEF sécurité globale,
- Sébastien DENEF : Chercheur, Fraunhofer Institute,
- Kevin HOY : Officier de Police, Great Manchester Police,
- Morgan MARQUIS-BOIRE : Ingénieur Sécurité , Google , conseiller technique du Citizen Lab de la Global Affairs de l'Université de Toronto.

Résumé des interventions :

Les réseaux sociaux jouent désormais un rôle important en cas de crise et tout spécialement dans le cadre de l'ordre public. En Royaume-uni, les réseaux sociaux sont désormais étroitement associés à la gestion de l'ordre public comme en témoigne l'exemple de la Police de Manchester. Il faut donc désormais considérer ces médias sociaux comme une aide et non comme un danger. En Europe, les Britanniques et les Néerlandais en sont un bon exemple

I. Problématiques

Il est nécessaire de déterminer le rôle des réseaux sociaux et d'évaluer dans l'absolu s'ils peuvent menacer l'ordre public dans nos sociétés. On pourra également mesurer la différence de niveau entre les pays européens en la matière et aborder les risques liés à cette exploitation des réseaux sociaux par les forces de police.

En terme d'ordre public, il est opportun de réfléchir sur les différents moyens à mettre en œuvre pour se servir au mieux des réseaux sociaux et s' en faire des alliés. Il ne faudra pas occulter les risques inhérents à cette utilisation.

Il apparaît également nécessaire de voir quels sont liens entre les médias sociaux, la sécurité et les droits de l'Homme. Le rôle des média sociaux dans le Printemps arabe et l'examen de l'exemple chinois permettent d'en mesurer le poids social et politique.

Dans le cas de l'exemple britannique, les analystes ont tenté de situer la portée de ces nouveaux moyens de communication dans le déroulement des émeutes de l'été 2011. On peut également se poser la question de savoir s'il est envisageable de se passer désormais de ces réseaux sociaux en terme d'ordre public.

II. Des solutions

Les réseaux sociaux sont des sources d'information pour la Police dans le cadre des enquêtes. Les forces de l'ordre peuvent également exister sur les réseaux sociaux. Ces derniers peuvent aider à montrer une police plus humaine et modifier les relations entre les citoyens et la police. Deux pays en Europe utilisent tous particulièrement les réseaux sociaux : la Grande Bretagne et les Pays bas. Les responsables des deux pays estiment que la police doit s'adapter aux changements médiatiques et de communication sachant que si la police n'est pas présente sur les réseaux sociaux d'autres le seront à sa place.

La police de Manchester est considérée comme pionnière en matière d'utilisation de réseaux sociaux et les utilisations sont nombreuses : renseignement d'ordre public, rassurer la population mais aussi recruter des futurs policiers. L'inscription de la Police sur les réseaux sociaux, sur Twitter principalement, a débuté en 2010 et ce, sans ligne de conduite précise. L'utilisation des médias sociaux a permis le début d'un dialogue entre la police et la population. Si, au début, les avis ont été assez partagés au sein de la police, force est de reconnaître que les réseaux sociaux ont été l'un de rares moyens mis à la disposition des policiers pour leur permettre de sortir de l'ombre.

Aujourd'hui la police de Manchester, qui compte 60 comptes Twitter et 60 comptes Facebook, ne pourrait plus se passer des réseaux sociaux. Les médias sociaux ont servi à éteindre des rumeurs qui circulaient sur le net. Ils se sont révélés des moyens d'informations plus rapides que des médias traditionnels comme la BBC. Dans le cadre de la gestion de l'ordre public, la Police a pu être au courant quasiment en temps réel de ce qui se passait au moment des pillages, Twitter a même servi pour identifier des émeutiers. Des risques existent cependant comme la fuite éventuelle de données. En effet, compte tenu de la contexture du net beaucoup d'informations arrivent dans des serveurs aux États-Unis et on note l'ouverture de faux comptes sous couvert d'une force de police. De plus les infrastructures des forces de police ne sont pas toujours à la hauteur en cas d'événement majeur.

La question du lien entre média et droits de l'Homme est pris en compte par l'Electronic Frontier Foundation (EEF), basée à San Francisco, qui travaille également à la question des droits numériques en ligne. S'agissant des pays arabes, il existe un consensus général pour dire que les réseaux sociaux ont été un acteur du Printemps arabe et que les utilisateurs ont été inventifs pour éviter les contrôles étatiques, comme en témoigne l'utilisation de fausses pages Facebook qui renvoient sur un site de l'opposition. Il est important également de souligner le rôle clé qu'apporte le contrôle des outils de communications. Quant au pouvoir chinois, celui-ci a les moyens de réagir aux média sociaux ; il a d'ailleurs mis en place Weibo, Twitter proprement chinois.

A21 - Droit du cyberespace : Entre réactivité et proactivité de la loi

Intervenants :

- Philippe VAN LINTHOUT : Magistrat, Belgique,
- Jacques GODFRAIN : Ancien ministre,
- Olivier ITEANU : Avocat au Barreau de Paris,
- Jan KERKHOFS : Magistrat, Belgique,
- Myriam QUEMENER : Procureur adjoint, responsable du pôle criminel, Tribunal de Grande Instance de Créteil,
- Bertrand WARUSFEL : Avocat, professeur à l'Université de Lille 2.

Résumé des interventions :

En 1988, la France s'est dotée d'une loi novatrice appréhendant les fondamentaux de la sécurité des systèmes d'information. Suffisamment générale, elle s'est pérennisée et s'inscrit dans un arsenal juridique relativement complet malgré un éparpillement des textes. La création d'outils juridiques pour lutter contre la cybercriminalité doit s'effectuer dans le respect des libertés publiques, tout en garantissant le principe de neutralité technologique. Cela permettra une connaissance plus claire de la loi par la population, même si d'autres problématiques, telles que la concurrence des normes sur le cyberespace et l'importante perfectibilité de la coopération internationale, semblent plus complexes à solutionner.

I. Naissance d'une loi novatrice

En 1987, les problématiques liées à la cybercriminalité n'étaient pas au centre des préoccupations. Personne ne voyait le danger et n'imaginait les sommes en jeu. C'est suite à un événement personnel que l'ancien ministre, Jacques Godfrain, alors Député, a pris connaissance des dérives liées au développement de technologies numériques. Il a alors initié la loi de 1988 relative à la fraude informatique et à la protection des systèmes de traitement automatisé de données. A l'époque, très peu de textes de lois prenaient en compte ces faits.

La loi Godfrain n'a pas été une liste d'infractions circonstancielles qui seraient aujourd'hui dépassées. Le véritable apport de cette loi réside dans le fait qu'elle intègre des dispositions prévoyant les fondamentaux de la sécurité des systèmes d'information que sont notamment la disponibilité, l'accès ou encore l'intégrité des données numériques.

II. État des lieux du corpus juridique français relatif à la cybercriminalité

Concernant le droit matériel, l'arsenal pénal français est plutôt complet. La plupart des dispositions classiques peuvent réprimer des faits liés à la cybercriminalité (fraudes, escroqueries, faux et usage de faux, etc.). Par ailleurs, des évolutions de circonstances aggravantes ont également été apportées (bande organisée, utilisation d'un réseau numérique, contrefaçon, etc.). De nouvelles incriminations ont plus récemment vu le jour, réprimant notamment le *Happy Slaping*[1], le *Phishing*[2] ou encore l'usurpation d'identité sur les réseaux sociaux.

1 - Le happy slapping ou vidéolynchage est une pratique consistant à filmer l'agression physique d'une personne à l'aide d'un téléphone portable. Le terme s'applique à des gestes d'intensité variable, de la simple vexation aux violences les plus graves, y compris les violences sexuelles.
2 - Le phishing est une technique utilisée pour obtenir des renseignements pour perpétrer une usurpation d'identité.

Le droit processuel relatif à la cybercriminalité a subi une accélération à partir de 2001. Ses liens avec la criminalité organisée, ou encore le terrorisme, ont imposé la mise en place d'avancées dans ce domaine. Il est possible de citer les interceptions téléphoniques étendues aux réseaux numériques, la possibilité de faire des copies ou de conserver des données, l'infiltration, la captation de données à distance pour les infractions les plus graves ou encore la création des juridictions inter-régionales spécialisées (JIRS).
L'arsenal pénal français est donc relativement complet malgré un éparpillement des textes. Il faudrait également une véritable politique pénale d'ensemble ainsi qu'un renforcement de la formation des magistrats pour ne pas rompre la chaine pénale.

III. Pro-action ou réaction de la loi face à la cybercriminalité

La pro-action et l'anticipation des menaces ne sont pas du ressort des législateurs mais plutôt des gens présents sur le terrain qui participent à la connaissance des nouveaux phénomènes. La loi doit arriver non pas en pro-action mais plutôt en réaction sous réserve de définir un équilibre entre les menaces et la sauvegarde des libertés publiques jointes à un impératif de sécurité publique.
Cela s'ajoute au principe de la neutralité technologique prescrivant qu'il ne faut pas faire une loi ciblée sur un phénomène technologique bien précis. En effet, par définition, la technologie est évolutive et le texte serait dépassé rapidement. L'exemple de la loi sur la cryptologie est flagrant, car complétement inutilisée du fait de son extrême spécialisation. Par ailleurs, il faut une collaboration efficace entre tous les acteurs d'internet. Créer une infraction pour sanctionner n'est pas efficace sur le cyberespace. Il faut privilégier une loi qui définisse des comportements et des statuts sur cet espace (exemple : responsabilité limitée des hébergeurs en contrepartie de la conservation des données de connexion).

IV. Limites de l'application de la loi dans le cyberespace

Plusieurs problèmes ont été identifiés. Tout d'abord, dans la société, peu de personnes connaissent réellement les conditions d'application de la loi dans le cyberespace. Cette dernière est devenue inaccessible pour le citoyen normal. Cela a favorisé la mise en place d'un véritable marketing de la peur et du service. En fait, la

loi semble absente du cyberespace.
Sur les réseaux numériques la loi est en concurrence avec d'autres normes qui régissent le comportement des individus, tels que l'environnement technique, les usages ou encore les lois d'un marché totalement privatisé.
Une autre problématique majeure, liée à l'application du droit dans le cyberespace, est la nécessité d'une adaptation des outils internationaux. En effet, la cybercriminalité s'inscrit dans l'internationalisation. Nous ne sommes jamais sûr de la nationalité des données saisies ni de leur lieu de stockage. En matière de cybercriminalité, la relative inefficacité de l'entraide judiciaire est constatée. Dans ce domaine, les délais de transmission des informations dépassent souvent les périodes de conservation des données. Il y a une nécessité de repenser l'approche vis-à-vis de la cybercriminalité pour se doter d'outils efficaces.
La Belgique, souhaitant être active dans ce domaine, s'est dotée de dispositions permettant d'agir unilatéralement sur décision d'un juge de façon à procéder en urgence à une perquisition sur un serveur situé potentiellement à l'étranger. La Belgique a pris le parti de déterminer que le Cloud est basé physiquement en Belgique, laissant à la charge des personnes poursuivies de prouver le contraire.

A22 - Usurpation d'identité : quels risques ? Quelles solutions ?

Intervenants :

- Cécile DOUTRIAUX : Avocate au barreau de Strasbourg,
- Jean-Paul PINTE : Maître de conférence (Université Catholique de Lille),
- Bruno CHAPPART : Directeur de la branche Authentification des personnes et des biens (Imprimerie Nationale),
- Mohamed CHAWKI: Conseiller d'Etat (Egypte), chercheur à l'Institut de Sciences Pénales et de Criminologie,
- Christophe CHARROT : Responsable fraude (FIA-NET),
- Philippe DEJEAN : Directeur technique division technologie et stratégie (Morpho).

Résumé des interventions :

Face à la multiplication des cas d'usurpation d'identité sur Internet (faux passeports, vol d'identité sur Internet, via les réseaux sociaux…), d'importants projets ont été lancés : CNIE, passeport biométrique, Idénum… L'interrogation porte sur les apports et les limites de ces technologies ou dispositifs, sur la mise en place d'une règlementation en la matière et de la capacité à prendre en compte une grande variété de données.

I. Les problématiques

Si la fraude à l'identité a toujours existé, on observe une forte augmentation de l'usurpation d'identité à hauteur de 40%. Les titres permettant d'identifier présentent des failles. Le nombre de circulations de données sur internet est très important. La mise en ligne de données personnelles sans discernement par des particuliers est un phénomène qui s'intensifie du fait de la dématérialisation électronique d'un grand nombre de procédures administratives et commerciales. Nos données personnelles ne sont pas seulement passées du support numérique au papier. Elles sont hors de portée sur des serveurs que nous ne connaissons pas. Nous avons perdu la maitrise de nos données personnelles, ce qui entraîne des risques de détournement.

La méthode utilisée par les délinquants pour s'approprier ces données peut se décliner en trois étapes : collecte des données, assemblage des données et, enfin, utilisation des données à travers la création d'un faux titre d'identité. Le plus gros point faible concerne les pièces justificatives utilisées pour la création d'une identité : factures, actes d'état civil. Ainsi, au moment de la création de l'identité, il n'y a pas de registre centralisé d'état civil. C'est une faille dans la structure qui permet l'usurpation

d'identité. Dès lors, il y a une réelle difficulté pour les agents publics à identifier la personne qui vient effectuer la demande d'une pièce d'identité. Cette problématique se retrouve sur internet avec les moyens de paiement à distance pour lesquels il est quasiment impossible de vérifier correctement l'identité du titulaire du moyen de paiement.
A cet égard, les groupes criminels procèdent à la construction de fausses identités numériques pour réaliser des actes d'achat, de vente ou des escroqueries. Les réseaux sociaux sont le principal centre de collecte des données personnelles par les groupes criminels. Ainsi, dans un internet social, les utilisateurs sont passés trop vite à une société de la connaissance et, surtout, ils n'ont pas conscience des risques inhérents à l'utilisation d'internet.

II. Des solutions

Elles passent par l'application des règles élémentaires de sécurité informatique. Ne pas converser avec des inconnus, car internet instille un climat de confiance propice aux échanges. Rapidement, l'utilisateur a tendance à confier des informations à caractère personnel à une tierce personne dont la qualité n'est pas établie. La meilleure façon de se protéger est de déterminer la stature de son interlocuteur.
Il faut changer régulièrement ses mots de passe et surtout dévoiler le moins possible d'informations nous concernant sur internet. En matière de sécurité bancaire, il ne faut pas hésiter à renforcer la sécurité du paiement sur internet auprès de sa banque (exemple : envoi d'un code de confirmation par sms).
La biométrie peut également être un moyen de sécuriser d'avantage les titres d'identité, puisque ces données propres à chaque être humain sont quasi-impossibles à falsifier. Néanmoins, on peut craindre un détournement de cette pratique de la part des états. Le rôle des autorités de surveillance comme la CNIL est donc à renforcer.
Les dernières réflexions conduisent à envisager une stricte authentification sur les réseaux numériques, avec une seule identité via une carte à puce biométrique d'identité. Néanmoins, ce projet ne suscite pas l'adhésion des populations.
La protection de son identité sur internet passe donc par l'application de règles simples visant à protéger ses données et son identité : en dire le moins possible, utiliser un antivirus et un pare-feu réseau, protéger ses moyens de paiement et se méfier des réseaux sociaux qui ne sont pas nécessairement sécurisés de façon ad hoc.

A23 - Outsourcing : comment externaliser en toute sécurité ?

Intervenants :

- Philippe HUMEAU : Président Directeur Général, NBS System,
- Yves LE FLOCH : Directeur du développement de la cybersécurité , Groupe SOGETI,
- Martine RICOUART-MAILLET : Avocat spécialisé en informatique, CIL et Auditeur Informatique & Libertés, BRM Avocats,
- Florent SKRABACZ : Responsable des Activités de Sécurité du Groupe , Steria.

Résumé des interventions :

Dans un contexte budgétaire restreint, les organisations cherchent à optimiser leur fonctionnement et réduire leurs coûts. Faut-il gérer en propre ou infogérer quitte à externaliser la gestion de certaines données sensibles au risque de ne pas disposer d'un niveau de sécurité optimal en matière de confidentialité, d'intégrité et de disponibilité.

I. Les problématiques

Le « *outsourcing* »[1] ou externalisation est un thème récurrent depuis ces dernières années du fait de la difficulté qu'éprouvent les entreprises à maîtriser des fonctions techniques, choronophages, onéreuses ou d'une évolutivité judirique forte.

1 - L'outsourcing est une pratique qui consiste à externaliser vers un prestataire spécialisé la totalité d'une fonction ou d'un service. C'est un service complet garantissant un même niveau de service au client.

La problématique concerne le contrôle d'une externalisation de fonctionnalités et de données sensibles sans que cette opération puisse induire une vulnérabilité et être la cause d'un préjudice pour l'entreprise. En conséquence, il importe d'analyser l'outsourcing comme une fonction de sécurité complexe du fait que la résolution et la prise en compte des problèmes de confidentialité et de vulnérabilité sont la base d'une confiance commerciale. La sensibilité de la donnée réside essentiellement dans la valeur ajoutée de celle-ci sur un marché concurrentiel et dans une concentration de la performance sur des tâches spécifiques. Ces valeurs doivent faire l'objet d'une sauvegarde particulière et impérative qui doit mettre en relation des acteurs fiables. Une piste de réflexion serait d'envisager la possibilité de labels pour les sociétés qui assureraient des externalisations : centres d'évaluation, prestataires de Cloud, etc.

En matière d'outsourcing, il apparaît opportun pour les responsables de la stratégie et le RSSI d'une entreprise de tenir compte des notions essentielles de dimension de liaison. L'externalisation suppose de confier des prestations à des sociétés sur un autre continent et de supporter des risques de non qualité. Il se pose aussi le problème de la localisation des données par le sous-traitant et de la cascade de sous-traitance. Il est utile de prendre en compte la

stipulation obligatoire ou facultative de clauses imposées voire des autorisations exigées par l'UE pour les données concernant les salariés notamment. On peut citer également les impacts du « *patriot act* » qui oblige toute société américaine ou européenne à dévoiler ce qui a trait à de l'espionnage ou des actes de terrorisme ce qui peut intéresser directement la protection de données personnelles détenues par l'entreprsise. L'obligation de non divulgation est caduque en matière de lutte contre le terrorisme.
Il importe également de situer le volume et la nature stratégique de données confidentielles. Il incombe donc aux entreprises intéressées de mettre en œuvre un arsenal de protection relativement important. Il combinera la mise en place de politique de formation et de sensibilisation interne avec la réalisation d'outils de protection informatique.

II. Les solutions

Les critères d'évaluation de la qualité de la prestation ainsi que les modalités de son évolution devront être définis contractuellement. Il convient également de définir les modalités de restauration du savoir-faire dans l'entreprise en cas de rupture de l'outsourcing.
En outre, il est possible pour les entreprises désireuses d'externaliser de mettre en œuvre en amont divers outils, tels que des audits, benchmarking et d'instaurer des pénalités, ce qui implique toutefois une dépendance par rapport au prestataire. La bonne gestion des risques passe par l'établissement d'indicateurs de performance (qualité, satisfaction-clients, fiabilité, respect des délais, investissement, innovation, taux de fréquence accidents...) qui seront mis en œuvre dans le cadre d'audits.

Il convient de considérer l'aspect juridique de l'outsourcing. En effet, plusieurs relations contractuelles sont possibles. Elles dépendent des moyens et des objectifs de l'entreprise. Le questionnement concerne le fait de procéder à une externalisation partielle ou complète. Suivra la détermination des modalités de la mise en place de l'outsourcing. Un cahier des charges pour définir le niveau de performances est souhaitable au même titre qu'une graduation de la valeur des données externalisées aux entreprises. Il est devenu fréquent d'inclure, dans les cas d'externalisation des systèmes d'informations, une clause sur les vulnérabilités logicielles ainsi que des pénalités financières. Enfin, on peut relever, dans la même perspective, la proposition de règlement européen prévoyant une notification des failles de sécurité relative aux données personnelles qui tend à devenir une obligation généralisée. Un des éléments juridiques majeurs est celui du partage de la responsabilité hébergeur / hébergé. En cas de litige l'entreprise externalisatrice, en marge du traitement, est tenue responsable en cas de mauvaise exécution ou de défaut d'exécution de ses obligations contractuelles.

A24 - Recrutement, formation et entraînement des professionnels de la cybersécurité

Intervenants :

- Charles Préaux : professeur des universités, fondateur et directeur de l'école d'ingénieurs en cyberdéfense au sein de l'ENSIBS,
- Yves-Tristan Boissan : général, commandant l'école des transmissions, ministère de la Défense,
- Sébastien Bombal : responsable de la majeure système, réseau et sécurité de l'Epita,
- Patrick Laclemence : directeur du centre de recherche de l'ENSP, professeur à l'université technologique de Troyes,
- Patrick Lallement : responsable du master SSI de l'université technologique de Troyes, responsable UTT du projet 2Centre.

Résumé des interventions :

A l'ère du tout numérique, la confiance revêt une importance croissante dans l'utilisation mondiale des réseaux informatiques. Une stratégie de cybersécurité (protection et maîtrise de l'information) est absolument nécessaire. Pour y parvenir, tant dans le secteur public que dans le secteur privé, il faut combler le déficit d'experts de la cybersécurité. Pour répondre à ce manque de vocations, de formations et d'entraînement, la stratégie serait de recruter et de former des spécialistes en sécurité des systèmes d'information au sein d'une véritable filière cybersécurité organisée avec ses différents métiers en un nouveau pôle d'excellence.

I. Une pénurie de talents

Dans le paysage du tout numérique, les défis de la cybersécurité restent difficiles à relever pour les états, notamment en France, par manque de ressources. Les formations existantes en sécurité des systèmes d'information (SSI) sont de création récente et ne répondent que partiellement à la montée en puissance d'une vaste problématique de cyberdéfense, de plus en plus prégnante (virologie, cryptologie, résilience des systèmes, gestion des crises). Tant dans le secteur public que dans le privé, les services ou les entreprises recrutent pour l'instant essentiellement en interne (périmètre DSI) avec des formations d'une durée moyenne de 18 mois mais peu variées. Le personnel qui suit ces programmes reste difficile à sélectionner

et n'est pas toujours disponible.
Les besoins sur le plan national sont clairement identifiés en trois niveaux et concernent la recherche d'ingénieurs (aux compétences pointues), la maîtrise des systèmes de veille des institutionnels (lutte contre la délinquance) et enfin la sensibilisation de la population (sur l'identité numérique). Ces besoins sont liés à une évolution vers une rapidité et une individualité de l'information et justifient une synergie entres professionnels et universitaires. Pour l'heure, il n'existe pas de lien entre le champ professionnel et une structure d'état à l'image de ce qui se pratique par exemple, pour la Santé publique[1].
Le manque de vocation constaté est pour l'essentiel lié à l'absence d'un parcours professionnel complet. Il s'agit de fidéliser les étudiants qui partent pour beaucoup dans les structures publiques[2] (ANSSI, MINDEF). Enfin, il s'agit d'instruire la totalité de la population pour acquérir les fondamentaux de l'espace numérique dans lequel elle se déplace aujourd'hui quotidiennement[3].

1- L'ensemble des filières est codifié (référentiel des emplois).

2 - Ceux-ci n'hésitent pas, par ailleurs, à faire des changements dans leur carrière, en l'absence de réelles filières de carrière.

Pour ces étudiants, de récentes actions de formation ont été mises en place et attestent de l'entrée progressive et de l'intégration du mot sécurité dans les universités. Une filière académique, ouvrant la porte à une jonction du professionnel et de l'universitaire, se dessine peu à peu.

3 - Inculquer une véritable « hygiène de sécurité ».

II. La prise de conscience et les ripostes

Dans le monde économique, le défi reste la sensibilisation à la veille, à l'intelligence économique (IE) en générant un développement d'outils de services sécurisés, point noir pour beaucoup d'entreprises. L'ensemble des stratégies de développement doit s'organiser tant pour la sécurité des applications que pour celle des systèmes industriels, avec un volet juridique dans les formations pour répondre aux incidents de sécurité (solution juridique, sûreté technique, informatique et des réseaux). Ce volet devra prendre en compte la complexité des différents régimes juridiques des pays, l'évaluation des préjudices, les étapes et les délais des procédures judiciaires (contentieux national et international).
La confiance dans le tout numérique ne sera possible que par le développement d'un partenariat fort entre l'État et le monde des entreprises, en favorisant toutes les synergies possibles (coûts humains et financiers.) La finalité consiste à mettre en place un corpus de formations qui fasse référence (référentiel de compétences et de métiers), offrant un panel de formations : en alternance au sein de l'entreprise, de validation des acquis d'expérience (VAE), diplômantes et qualifiantes.
La stratégie vise le développement d'un véritable *sociologie opérationnelle, intuitive et transverse*, en répondant à la fois à la cybersécurité, à la cybercriminalité et la cyberdéfense. L'objectif est de couvrir le champ de la SSI (protection), la cybercriminalité (détection) avec le traitement des incidents et l'analyse et la cyberdéfense (pour les services de l'État, protection de systèmes sensibles et conséquents).
La mise en place de ces différents métiers regroupés au sein d'une véritable filière cybersécurité donnerait naissance à un vrai pôle d'excellence, seul moyen véritablement efficace pour générer et protéger la confiance numérique au quotidien.

A25 - Les Collectivités Territoriales face aux risques numériques

Intervenants :

- Lieutenant-Colonel Rémy Février : Chargé de mission Intelligence Economique à la Région de Gendarmerie Nord-Pas de Calais, Docteur en Sciences de Gestion, Qualifié aux fonctions de Maître de Conférences, Professeur – associé à l'Université Paris I – Panthéon Sorbonne.

Résumé des interventions :

Cette intervention s'est structurée autour de la présentation des travaux scientifiques du lieutenant-coloenl Rémy Février relative au management de la Sécurité des Systèmes d'Information en Collectivités Territoriales.

I. Vulnérabilités des SI Institutionnels

Si l'ensemble des acteurs publics et privés appréhende globalement la notion de *virus* informatiques, rares sont les non-spécialistes disposant d'une vue d'ensemble des dangers que courent les institutions et entreprises modernes au travers de leur systèmes d'information. Toutes les entreprises et institutions modernes constituent des cibles potentielles d'attaques informatiques. La diffusion des TIC ainsi que le niveau de technicité atteint par les cyberpirates, font des collectivités des cibles de choix car souvent insuffisamment protégées. Dans le cas d'une collectivité territoriale de taille respectable, on peut très bien envisager, par exemple, une attaque ciblée d'internautes contrariés par une décision ayant trait à la qualité de vie ou aux élections. Si ce genre de menaces peut légitimement sembler peu crédible à un non spécialiste, il n'en demeure pas moins que l'évolution constatée du *hacking* en général, et de la personnalité de certains pirates militants en particulier, ne peut qu'inciter à la prudence et à la mise en place d'une politique de SSI.

Il existe trois principaux types de malware susceptibles de compromettre le bon fonctionnement d'un SI, voire d'en extraire frauduleusement des informations stratégiques. Les pirates individuels *hackers* sont le plus souvent des passionnés d'informatiques, maîtrisant parfaitement les principales failles des différents types de réseaux existants, qui se répartissent en quatre catégories selon le but recherché[1].

Pour autant, il serait erroné de voir en chaque pirate un individu

1 - Les « whites hats » (chapeaux blancs) dont l'objectif est de détecter les vulnérabilités des SI et d'en avertir les administrateurs réseaux afin d'améliorer la sécurité de ceux-ci.

- Les « blacks hats » (chapeaux noirs) qui pénètrent les systèmes afin d'en tirer un bénéfice personnel.

- Les « greys hats » (chapeaux gris) qui, comme leur nom l'indique, se situent à mi-chemin des deux catégories précédentes.

- Et les « hacktivistes », contraction des mots « hackers » et activistes qui agissent dans un but purement idéologique.

isolé membre d'une communauté *underground* solidaire. En effet, les menaces peuvent également provenir d'autres horizons, à l'image du crime organisé, des services de renseignements étrangers ou encore, dans le cadre du secteur marchand, de concurrents peu scrupuleux. Parallèlement à la pénétration des SI à des fins crapuleuses, se développe de plus en plus l'atteinte orchestrée par des services étatiques étrangers agissant en fonction de l'actualité ou d'objectifs précis. Ainsi, la pénétration d'institutions nationales ou internationales devient monnaie courante, que ce soit à des fins de récupération de données d'importance vitale ou dans une optique beaucoup plus militaire de paralysie des SI stratégiques.

On peut légitimement supposer que les SI des collectivités territoriales deviendront de plus en plus des cibles comme les autres, au fur et à mesure que ces dernières intégreront les nouvelles technologies dans leurs processus de gestion des flux informationnels. Malheureusement, du moins en ce qui concerne notre pays et en dépit de certains avertissements régulièrement lancés par les services territoriaux d'Intelligence Economique (IE), notamment de la Gendarmerie Nationale, cet état de fait reste encore bien trop ignoré des décideurs locaux et le plus souvent des pouvoirs publics dans leur ensemble. L'on constate ainsi des prises de contrôle à distance d'un ordinateur cible, de la collecte d'informations confidentielles[2], des compromission de systèmes et usurpation d'identité (les données à caractère personnel deviennent une cible de choix, soit directement soit indirectement, ces informations pouvant ainsi conduire à des délits de vols d'identités). Parallèlement, il est aisé de relever également, par analogie, la vulnérabilité potentielle des grandes administrations de l'Etat dont une partie de l'activité intrinsèque consiste en un archivage méticuleux de grandes quantités d'informations d'ordre strictement personnel : Trésor Public, hôpitaux, Sécurité Sociale etc.

2 - Alors que ces attaques concernent le plus souvent des entreprises et des particuliers, elles deviennent de plus en plus complexes et devraient, tôt ou tard, toucher les collectivités territoriales, maillon indispensable au bon fonctionnement de notre pays et sources premières de données personnelles susceptibles d'être vendues ou utilisées comme vecteurs d'attaques informationnelles.

II. Un phénomène nouveau : les attaques contre les collectivités territoriales

Un phénomène totalement nouveau est apparu depuis deux ans : l'intrusion dans les SI des collectivités territoriales. S'il s'avère extrêmement difficile de disposer de données quantitatives à ce sujet, du fait de la prudence compréhensible dont ces dernières font preuve, de plus en plus d'attaques deviennent néanmoins publiques, notamment du fait de l'appétence de journalistes de plus en plus sensibilisés à ce genre de menaces. Sans remonter outre mesure dans le temps, force est de constater que les atteintes aux systèmes d'informations n'épargnent plus les collectivités territoriales, que ce soit en France ou à l'étranger.

Le premier type d'attaque informatique revient à la pénétration d'un SI d'une collectivité depuis l'extérieur. Nous relèverons, à ce propos, un exemple particulièrement symptomatique de compromission de systèmes mettant en cause une grande ville : la ville de Reims (51) a subi dans les premiers jours de mars 2011, une attaque de type pénétration directe via un flux RSS[3]. Révélé par la presse locale, il semble que les pirates aient profité d'une faille de sécurité spécifique.

Pour comprendre cette problématique, une enquête a été réalisée

3 - Flux RSS (Really Simple Syndication) : format particulier de données, constamment mis à jour et visant à diffuser automatiquement des informations à l'intention des internautes selon un principe de « fil d'actualité ».

grâce à une opportunité liée à la volonté de la Région de Gendarmerie Nord-Pas-de-Calais et du Conseil Régional de conjuguer leurs efforts en matière de sensibilisation des décideurs territoriaux aux menaces numériques a permis, en s'appuyant sur un maillage territorial sans équivalent (1547 communes, regroupés en 91 établissements publics de coopération intercommunale) d'obtenir les résultats suivants et en déduire les pistes d'amélioration.

L'ensemble des traitements statistiques effectués (tris à plat, tris croisés et statistiques complexes) montre que le management de la SSI par les collectivités territoriales françaises demeure très nettement insuffisant, a fortiori dans les collectivités territoriales les plus modestes, qui en représentent la très grande majorité. Il apparaît que les pistes d'amélioration sont :

- La désignation d'un Responsable de la Sécurité des Systèmes d'Information. Pour se protéger d'une mise en cause de sa responsabilité, le dirigeant public doit impulser une réelle politique de sécurité des réseaux informatiques
- la nomination d'un Correspondant Informatique et Libertés. Les collectivités territoriales étant des entités publiques, elles se doivent de respecter l'ensemble des obligations qui leur sont faites relativement à l'utilisation d'un SI, a fortiori en ce qui concerne le traitement, la gestion et les conditions de conservation de données à caractère personnel. Or, la CNIL, soucieuse de favoriser un dialogue constructif avec l'ensemble des entités publiques et privées, a mis en place la possibilité, pour n'importe quelle organisation publique et privée, de désigner un Correspondant Informatique et Libertés (CIL). La nomination de ce dernier, en plus de représenter un geste de bonne volonté de la part de l'entité concernée, permet également d'alléger le dispositif de déclaration des fichiers informatisées les plus courants et comportant des données à caractère personnel. Toutefois, l'existence d'un CIL n'exonère pas le dirigeant qui demeure, dans tous les cas, le responsable des traitements.
- la mise en place d'une Politique de Sécurité des Systèmes d'Information. Si l'ensemble des tâches incombant au RSSI est fort étendu, l'une de ses priorités devra être de proposer, aux dirigeants de la collectivité, une Politique de Sécurité des Systèmes d'Information (PSSI) puis d'assurer sa mise en place opérationnelle.

Bâtissez votre Cloud sur du concret

OVH fournisseur d'infrastructure Internet

9 Datacentres - 33 Points de Peering - Réseau mondial en fibre optique

Le meilleur du réel et du virtuel

www.ovh.com/pc

Plus d'informations

Domaine | E-mail | Hébergements mutualisés | VPS | Serveurs dédiés | Private Cloud | Cloud | ADSL | VoIP | SMS & Fax

OVH.COM/pcc

contactez-nous **09 72 10 72 10**

Lun - Vend : 9h - 18h | Prix d'un appel local

Digiposte
entreprises

QUAND UNE SOLUTION SIMPLIFIE LA VIE DE VOS CLIENTS, ÇA SE VOIT !

Relevés de compte, points fidélité, factures... Avec DIGIPOSTE, vous avez la solution pour inciter vos clients à adopter une réception numérique et 100 % sécurisée de leurs documents. Mais aussi de bénéficier de services à valeur ajoutée (photos certifiées, alertes de paiement...).
Ainsi, vous êtes certain de simplifier le quotidien de vos clients !

Plus d'infos sur www.laposte.fr/digiposte/entreprises

www.laposte.fr

LA POSTE | SOLUTIONS BUSINESS

B1 - Cyber terrorisme : mythe et réalité

Intervenants :

- Stéphane TIJARDOVIC : commissaire divisionnaire, ministère de l'intérieur,
- Nicolas ARPAGIAN : INHESJ rédacteur en chef de la revue Prospective Stratégique,
- Sylvain JOLY : Ministère de l'intérieur, Direction générale de la police nationale (DGPN),
- Jarno LIMNEL : Société Stonesoft (Ancien militaire finlandais),
- Andrea RAFFAELLI : Arme des Carabiniers (Italie),
- ROMERO RAMOS : Guardia Civil (Espagne).

Résumé des interventions :

Pour le moment, le cyberespace est plutôt considéré comme un instrument et non comme une cible pour la réalisation d'actes terroristes.
Pourtant, certaines mouvances terroristes (Al Quaeda) auraient aujourd'hui les capacités techniques de mettre en œuvre des attaques sur les systèmes informatiques. Les réseaux ne sont pas encore assez interconnectés pour déstabiliser les activités d'importance vitale, les terroristes ne s'intéressent pas encore à ce type de cible.
Il faut réaliser un équilibre entre la mise en œuvre de pouvoirs d'enquête et de surveillance qui sont exorbitants du droit commun et le respect des libertés publiques. Toute systématisation risquerait de rendre aveugle par saturation les services de renseignement. En outre, il n'y a pas de volonté des Etats de permettre le traçage des cyberattaques, car ce mode opératoire permet d'avancer masqué sans risque politique ou juridique.
L'avenir semble appartenir au cyberterrorisme. Après les attentats du 11 septembre, les attaques sur le monde physique sont en déclin mais il faut être convaincu qu'il y aura des attaques « cyber » que l'on ne saura pas empêcher. La doctrine en matière de cybersécurité serait de chercher à réduire l'impact de celles-ci plutôt que de chercher à construire une « ligne Maginot » issue de *scenario* improbables.

I. Etat des lieux

Selon l'article 421-1 du code pénal français, sont des actes de terrorisme certaines infractions, (notamment celles qui portent atteinte aux systèmes automatisés de traitement de données) ayant pour but de troubler gravement l'ordre public par l'intimidation et la terreur. Cette définition peut-elle être applicable au cyberespace? Si notre définition nationale est claire, la définition internationale donne lieu à des controverses, certains qualifiant d'actes de « *résistance* » des faits qui pour d'autres relèvent

du terrorisme. Il n'existe pas de définition du cyberterrorisme au sein de l'Union européenne bien qu'une décision-cadre de 2002, amendée en 2008, définisse un cadre d'action pour la lutte contre le terrorisme. Au sein de l'ONU, un guide, publié en octobre 2012, définit le cyberterrorisme comme « *l'utilisation d'internet pour la propagation d'infractions terroristes* ».
Le cyberterrorisme reste un concept flou du fait de la dématérialisation. Le cyberespace est souvent considéré comme un instrument et non comme une cible pour la réalisation d'actes terroristes. L'interconnexion des réseaux favorise le lien entre terrorisme et informatique. Il est établi qu'internet est aujourd'hui un moyen utilisé par les différentes mouvances pour communiquer, faire du prosélytisme, de la propagande, donner des instructions cryptées ou transmises par stéganographie. Il peut être un moyen de terreur lorsqu'il véhicule des contenus généralement censurés par la presse (images insoutenables de mise à mort d'otages). Internet facilite également les transferts financiers, sans lesquels des attentats ne pourraient être organisés.

II. Perspectives

Pour l'heure, aucun acte ayant des conséquences physiques (mort d'hommes, destructions) n'a été recensé. Le cyberterrorisme actif prendrait la forme d'une attaque massive sur les systèmes informatiques qui pourrait avoir pour conséquence une désorganisation de la vie de la société en visant des infrastructures critiques : banque, finance, énergie, transports, santé, etc… Les attaques contre les installations nucléaires iraniennes à l'aide du virus STUXNET ouvrent une nouvelle ère, même si elles ont été imputées par les observateurs à des services relevant d'états. Les faits que l'on pourraient qualifier de cyberterrorisme proviennent pour le moment d'entités qui ne sont pas terroristes à l'origine. La paternité des actes n'est jamais reconnue et leur imputabilité bute sur les moyens d'investigation et l'extraterritorialité. Il n'y a pas de volonté des états de permettre le traçage des cyberattaques, car ce mode opératoire permet d'avancer masqué sans risque politique ou juridique.
Les terroristes progressent dans leur maîtrise informatique. Leurs ressources financières leur permettraient, s'ils en avaient l'intention, d'acheter des moyens ou des services, de mobiliser des capacités techniques pour mener des attaques sur les systèmes informatiques. Si la convergence vers le « *tout IP* » met en évidence des fragilités, notamment au sein des infrastructures critiques, les réseaux ne sont pas encore assez interconnectés pour déstabiliser les activités d'importance vitale. En conséquence, les terroristes ne s'intéressent pas encore à ce type de cible mais on doit noter l'émergence du concept de « *cyber-guerilla* » : la menace est diffuse et peut être perpétrée par des groupes d'individus restreints, voire des isolés.
La difficulté dans la lutte contre le cyberterrorisme est de réaliser un subtil équilibre entre la mise en œuvre de pouvoirs d'enquête et de surveillance, qui sont par définition exorbitants du droit commun, et un contrôle accru des systèmes d'information. Le contrôle systématique par les gouvernements des communications de « *la grande masse des gens* » serait disproportionné par rapport à un péril terroriste encore « *nébuleux* ». Les services spécialisés ne sont pas forcément favorables au contrôle et à la surveillance totale des réseaux, via des mots clés, qui ne serait pas durablement efficace face aux stratégies de contournement qui pourraient être mises en œuvre.
Il faut être convaincu que l'on ne saura pas empêcher certaines attaques. La doctrine en

matière de cybersécurité aurait pour objectif de chercher à réduire l'impact plutôt que de chercher à construire une « *ligne Maginot* » issue de scénario improbables. L'idée est de réduire l'impact des dysfonctionnements par le développement d'une capacité de résilience. Dans ce domaine, il n'y aura jamais de solution offrant une protection absolue.

Depuis le 11 septembre 2001, les attaques dans le « *monde physique* » diminuent. L'émergence d'un cyberterrorisme ayant des conséquences humaines et matérielles est possible. La menace repose sur les vulnérabilités au sein de chaque pays, les capacités de résilience et la volonté des terroristes. Au-delà des capacités développées au sein de chaque Etat, la coopération internationale est plus que jamais nécessaire.

B2 - Sécurité des télécommunications

Intervenants :

- Ariel Gomez : rédacteur en chef, Journal Des Télécoms,
- Laurent Maynard : responsable du business développement sur le marché défense, Alcatel-Lucent,
- Constant Hardy : commissaire aux communications électroniques de défense, ministère de l'Economie et des Finances,
- Marc Lefèbvre, Orange Consulting,
- Raphaël Marichez, fonctionnaire de la sécurité des systèmes d'information , ministère de l'Intérieur.

Résumé des interventions :

La sécurité des systèmes d'information (SSI) ne repose pas uniquement sur la sécurité des données, des applications et du réseau d'entreprise. A l'heure du développement de l'informatique en nuages (cloud computing), la SSI est indissociable des infrastructures de télécommunication mises en œuvre et utilisées par les opérateurs. Fournisseurs d'un produit, il incombe à ces derniers de s'assurer de la sécurité des équipements réseaux. Enfin, en matière de télécommunication, la sécurité mise en place doit être suffisante pour garantir et développer la confiance entre les différents partenaires.

I- Etat des lieux

La sécurité des télécommunications est étroitement liée à la sécurité des équipements « *réseaux* ». Les derniers travaux publiés montrent qu'en France la résilience de l'internet a atteint un niveau acceptable. Cependant une vigilance de chaque instant est de mise dans la mesure où internet a pris une place telle dans les activités et l'économie du territoire qu'il reste sensible à la moindre menace. A ce titre, la France occupe une position « *originale* » puisque, avec cinq opérateurs « *grand public* » qui développent leurs propres infrastructures, la concurrence dans le domaine des communications électroniques est une réalité concrète et effective.
Pour leur part, les équipementiers contribuent, eux aussi, à renforcer cette résilience d'une part en intégrant la notion sécuritaire dès la conception de leurs produits et, d'autre part, en maintenant une recherche permanente en cybersécurité afin d'être en mesure d'anticiper ou de réagir dans l'hypothèse d'une panne ou d'une attaque. En cas d'incident, il convient de distinguer le seuil critique (qui touche le réseau) de celui du reste de l'internet (périphériques). Les pannes majeures sont souvent générées par de grosses intempéries (ouragans,

black-out électronique) et les réseaux de secours permettent généralement de garantir la transmission des données. Ainsi, la majorité des réseaux (hertziens ou terrestres), ne reposant pas sur Internet, reste opérationnelle.
La menace constituée par le risque d'un sabotage physique des réseaux est prise en compte et intégrée par les opérateurs, lesquels doublent bien souvent leurs capacités avec des systèmes de secours. Mais la crainte principale réside dans une standardisation excessive des protocoles. Pour les développeurs, elle peut certes répondre à des intérêts économiques, mais son extension à grande échelle constitue un risque de fragilisation des réseaux en cas d'attaque à visée terroriste. Aussi, les responsables SSI (administrations, ministères, entreprises...) sont très attentifs à ces évolutions. Si les surveillances exercées mettent à jour l'existence d'opérateurs utilisant le même produit, des points de concentration, ou encore une redondance dans la configuration de logiciels ou d'équipement, les clignotants passeront rapidement à l'orange.

II. Perspectives

Pour les raisons évoquées précédemment, il est primordial que les opérateurs développent une gamme de moyens de protection et d'intervention qui diffère selon la « *force* » du coup porté : il va de soi que les mesures de sécurité prises n'auront pas la même portée si c'est tout un réseau, avec ses milliers de machines, qui est visé (attaque de nature terroriste) ou si l'incident est de niveau moindre (attaque commerciale ou espionnage).
En terme de fiabilité, les opérateurs ont conscience des enjeux et prennent les dispositions nécessaires pour limiter les effets. On ne compte qu'une grosse panne par an en France et une panne majeure mondiale tous les deux ans, causées bien souvent par une erreur humaine de manipulation ou d'exploitation. S'agissant de la sécurité des communications, notamment par téléphone et SMS, ces vecteurs se piratent facilement et le choix des autorités reste majoritairement de ne pas s'appuyer sur ce type de vecteurs, en particulier pour les communications opérationnelles.
Dans la sphère économique, les entreprises basculent de plus en plus vers le cloud computing, un concept reposant sur la mutualisation des ressources qui permet de mettre à disposition le même service à plusieurs clients, en s'appuyant sur les mêmes équipements physiques.
Ce concept n'est pas sans présenter un risque, notamment par la concentration des systèmes et des données dont le stockage dans des zones de centralisation peuvent faire l'objet, surtout si elles sont sensibles, de convoitises. Sur la toile, des risques subsistent comme ceux de la gouvernance (transfert de la surveillance), du maintien de la visibilité, de la confidentialité (serveurs à l'extérieur), de la disponibilité des réseaux et également de leur traçabilité. Les opérateurs pour y répondre développent un maillage mondial et national.
Les moyens matériels utilisés pour les réseaux (infrastructures en fibre optique) peuvent aussi constituer des « *porosités* » et favoriser l'écoute du signal optique pour détecter une interruption ou une action. En effet, il est possible de récupérer des données quand les fibres sont courbées, entraînant de ce fait la propagation de rayons à fuite dans la gaine.
Dans ce contexte général, les objectifs sont d'éviter au mieux les vulnérabilités en garantissant la mise en œuvre de plusieurs technologies différentes (équipementiers, réseaux), de s'accorder sur une standardisation des interfaces tout en maintenant une nécessaire diversité au cœur

de l'appareil et des réseaux.
Pour les entreprises qui ne sont pas toujours informées de ces risques, il est indispensable que de véritables synergies d'interopérabilité se développent en s'appuyant sur des rencontres régulières entre industriels concepteurs et utilisateurs.

B3 - Plans de continuité et reprise d'activité : la question du retour en mode dégradé

Intervenants :

- Claire BERNISSON : Consultante en Sécurité et Gestion des Risques, LEXSI,
- Emmanuel WINCKLER : Expert sécurité SOGETI ESEC,
- Paul THERON : Expert en cyber-résilience et en gestion de crise, Thales,
- Philippe VILANDRAU : Directeur des opérations, Voyages SNCF.com.

Résumé des interventions :

Les plans de continuité et de reprise d'activité concernent un ensemble de process déterminés de concert par le RSSI et le responsable de ces plans. Ils visent la restauration programmée des fonctionnalités et des métiers d'une entreprise. Ces plans nécessitent une analyse fine des fonctionnalités et des besoins de l'entreprise, un plan de formation à la réaction à l'événement et une formalisation étroite des chaînes de responsabilité et de la synchronisation des réponses opérationnelles.

I. Domaine des plans

Le PCA, plan de continuité d'activité, vise la continuité de l'activité de l'entreprise, du moins dans son coeur de métier essentiel, tout en supportant un seuil de dégradation acceptable des processus au regard de la résilience du système. Il comporte une problématique essentielle de la protection de la donnée. Il comprend un ensemble de procédures qui balaient les matériels, les réseaux et les attributions des personnels selon leurs postes. Il intègre une analyse des besoins réels des services et l'intégration des projets à long terme de l'entreprise.

Le PRA vise à permettre la reprise de l'activité dans sa globalité ou en mode dégradé. Les procédures doivent prendre en compte l'ensemble des infrastructures et des réseaux associés. Elles peuvent s'appliquer à des serveurs, à des des infrastructures distribuées sur plusieurs sites et intéresser des milliers d'équipements. Une entreprise ayant une activité à l'international devra tenir compte de la diversité des cultures de ses opérateurs.

Les opérations, consécutives à une crise majeure concernant un centre informatique, organisent le reconditionnement de l'infrastructure, la remise en route des applications sur site natif ou sur un site de secours et la vérification de l'intégrité des processus démarrés en mode dégradé.

La problématique de l'incitation des entreprises à mettre en place un PCA/PRA est majeure. On note toutefois que de nombreux sujets

exposés tels que les banques[1], les sites de vente en ligne etc. ont tendance à se montrer réticents à la réalisation de ce type de dispositifs préventifs et curatifs. Le fait que l'assureur ne couvre que le risque aléatoire peut également expliquer l'hésitation exprimée par les professionnels à la mise en place d'un PCA /PRA. Il est toutefois constaté que la mise en oeuvre d'un PCA s'avère bénéfique pour l'entreprise. Elle est l'occasion de revisiter des processus métiers, de les simplifier et d'accroître la productivité.

1 - Il faut toutefois noter que la réglementation CBRF 2004-2 (issu de IASB-Bâle II) rend obligatoire un plan de secours opérationnel pour les établissements financiers, banques et assurances.

L'exemple de la gestion du site « *Voyage-SNCF.com* » permet d'aborder une autre problématique liée à l'ouverture à la concurrence et au traitement des données ouvert à des tiers. Cet aspect est critique si l'on prend en compte le fait de 1800 interventions techniques annuelles. Le Système de PCA est donc coûteux et parfois incomplet, en matière de cybercriminalité notamment.

Il faut rappeler l'importance de la norme « *iso 22320* »[2] qui prépare la certification des organisations en matière de PCA/PRA. Elle établit les interactions entre les opérateurs en charge de la gestion de crise, les méthodologies pour sérier les processus utiles et les informations vitales aux opérations de maintenance ou de restauration des applicatifs et des infrastructures.

2 - L'ISO 22320:2011 détermine le cadre opérationnel, le suivi des opérations et les termes de la coopération entre des acteurs de la crise. Elle traite de la traçabilité, de la gestion des informations et de l'interopérabilité. Elle spécifie les processus, les systèmes de travail et les modalités de saisie et de gestion des données. Elle peut-être appliquée à tout organisme qu'il soit privé ou public.

II. Des solutions

Le PRA doit spécifier dans un référentiel le cadre de la gestion humaine du risque. Il définit les responsabilités des personnes de l'entreprise concernées. Elles doivent donc être désignées et détenir les informations et la formation utile à leur réaction opérationnelle.

Le PRA est réalisé au regard d'une configuration logicielle et d'infrastructure de l'entreprise. En conséquence, la modification du parc doit être régulièrement répercutée dans le plan. Les applications doivent être évaluées pour déterminer leur vulnérabilité et les traitements curatifs qui doivent être mis en place en cas de crise. Cette analyse permet de lister dans des documents normés les besoins en matière de sauvegarde et de restauration des données mais également des logiciels des serveurs et des automates.

Il faut également intégrer l'impact d'une indisponibilité de la fonctionnalité et déterminer son point « *létal* » quant aux autres applicatifs qui s'appuient sur elle. Il s'ensuit la détermination de priorités dans la reconstruction des applicatifs. On ne peut ignorer que la qualité de cette analyse permettra une limitation des coûts lors de la contractualistion d'opérations de maintenance externalisées. La synchronisation des environnements de sauvegarde et de restauration doit être établie de façon à permettre une mise en oeuvre maîtrisée et vérifiable par phases.

Certaines entreprises ou administration, au vu de la sensibilité de la donnée ou de l'obligation d'une continuité des services ont prévu la construction d'un site distant homothétique qui va prendre le relais du site principal déficient. Les mises à jour logicielles, les maintenances et l'interopérabilité des personnels et des matériels mises en oeuvre doivent être indentiques. Des exercices et simulations doivent être menés régulièrement. Cela nécessite la construction de *scénario* de crise mettant en oeuvre non pas une suite « *non réaliste* » d'incidents mais des chaînes d'incidents visant à valider des réponses essentielles et normées. Les documents doivent être corrigés après un retour d'expérience validé par des réunions croisées.

B4 - Cybercriminalité bancaire et financière

Intervenants :

- Gilles DELILLE : directeur sécurité des systèmes d'information, groupe Crédit Agricole,
- Myriam QUEMENER : Procureur adjoint, responsable du pôle criminel, tribunal de Grande Instance de Créteil,
- Régis ROCROY : consultant SSI,
- Pierre CHASSIGNEUX : Directeur risk Management & Audit, Groupement des cartes bancaires,
- Daniela TRICCA : R.A.C.I.S, Italie.

Résumé des interventions :

La cybercriminalité bancaire est en croissance favorisée par les paiements à distance, et notamment sur le canal Internet. Elle exploite des modes opératoires originaux et complexes qui ne connaissent aucune limite territoriale. Sa nature par définition virtuelle favorise aussi de nouvelles formes plus complexes pour les procédures de blanchiment.
Les mesures prises à l'encontre de cette cybercriminalité bancaire sont de deux ordres. L'innovation technologique et la sensibilisation des acteurs à l'utilisation de ces nouvelles méthodes sont un premier pare-feux. Le second réside dans les réponses des institutions en termes d'échanges d'informations et d'harmonisation juridique et technique.

I. Les problématiques

Le volume financier des fraudes s'estime bien sûr en fonction de la valeur des transactions globales mais l'appréciation des préjudices s'attache aussi à la ventilation des actes délictuels.
Selon le rapport de l'Observatoire de la sécurité des cartes de paiement de la Banque de France, le montant de la fraude à la carte bancaire représente 413,2 millions d'euros en 2011. En Europe, le montant cumulé des fraudes en 2010 se situe à 1,26 milliard d'euros. La majeure partie de ces fraudes se concentre sur les paiements à distance et, plus particulièrement, en matière de paiement sur internet. En terme de typologie de fraude, le numéro de carte bancaire usurpé arrive en tête avec 59,9 % des cas constatés, devant la carte perdue ou volée à 36,1 %. La fraude à la carte bancaire est possible selon trois modes opératoires : l'utilisation par un tiers d'une carte perdue ou volée, la contrefaçon d'une carte ou l'utilisation des identifiants de la carte (numéro, date d'expiration…) par une autre personne que son titulaire. Les cas de contrefaçon concernent la piste magnétique de la carte. En effet, la reproduction de la piste peut permettre une utilisation frau-

duleuse dans les pays où la technologie de la carte à puce n'est pas utilisée. La copie de la piste magnétique - soit par une personne malveillante, soit grâce à un dispositif placé sur le terminal de paiement ou sur le DAB - est connue sous le nom de "*skimming*".

Le volume de la fraude transfrontière est supérieur à celui de la fraude domestique. Ainsi, en 2010, on observait 25% de fraudes pour 2% de paiements transfrontaliers acquis hors espace SEPA[1]. Les niveaux de fraude sont moins élevés dans la zone euro que dans l'Espace unique des paiements en euro. Une analyse des flux de paiement dans et hors de l'Espace unique de paiement en euro démontre que la fraude à la carte de paiement est une activité organisée à l'échelle internationale qui nécessite des mesures de prévention concertées et des normes internationales, comme le standard EMV ou une authentification plus forte en le combinant avec 3D Secure.

1 - L'Espace unique de paiement en euros, en anglais Single Euro Payments Area (SEPA).

La cybercriminalité financière doit aussi être considérée sous l'angle des détournements des flux financiers. Sur l'internet, en raison notamment de la multiplication des banques en ligne, des casinos virtuels, des sites de paris en ligne et des possibilités de placements boursiers en ligne, les possibilités de blanchiment d'argent sont illimitées. Ainsi, transférer des capitaux sur le web est devenu une activité fleurissante. Les intermédiaires recrutés sont qualifiés de «mules» et peuvent gagner une somme d'argent considérable, en toute illégalité. Avec ces modes opératoires, les activités cybercriminelles demeurent incontrôlables et les poursuites en justice se révèlent parfois impossibles. Les diverses mafias se sont logiquement tournées vers la Toile pour l'activité de blanchiment de l'argent. D'abord, la monnaie virtuelle joue un rôle central dans le fonctionnement des black markets. Elle est insaisissable, difficile à tracer et permet aux cybercriminels, en leur garantissant. l'anonymat, d'effectuer leurs transactions sans risque. Mais les bénéfices des ventes sur les marchés noirs de la cybercriminalité ne restent pas longtemps virtuels. Le vendeur devra, pour récupérer le résultat de ses ventes, faire appel à différents acteurs.

L'économie souterraine de la cybercriminalité possède, comme pour le trafic de drogue, ses propres mules. Il s'agit d'individus recrutés via l'internet pour servir d'intermédiaires afin de récupérer les fonds illicites. En contrepartie des opérations de transferts de fonds dont elle aura la charge, la mule reçoit à titre de commission entre 5 et 10% du montant transféré. Les fonds en question sont retirés par la mule sous forme de liquide après les avoir reçus sur son propre compte bancaire et renvoyés par la suite aux cybercriminels à l'aide de services de transfert d'argent, comme la Western Union par exemple. La cybercriminalité rejoint dès lors la criminalité classique qui utilise aussi majoritairement ces deux procédés afin de blanchir l'argent issu d'activités frauduleuses.

II. Cohésions transnationales technologiques et policières

Pour lutter efficacement contre la fraude, il est nécessaire de bénéficier d'un maximum d'informations et d'opposer des pare-feux technologiques toujours plus efficients. La disparité des niveaux de sécurité des opérations bancaires selon les pays fragilise fortement la sécurité globale. Seules 13% des transactions menées sur le territoire français sont protégées contre les fraudes à la carte bancaire et au vol de données personnelles alors que le taux de protection va

au-delà de 95% dans certains pays comme le Royaume-Uni.
Les banques renforcent en permanence la sécurité des systèmes de paiement et des sites de banque en ligne dont les dispositifs d'authentification forte, les dispositifs d'authentification à code non rejouable (code unique envoyé par SMS, généré par une calculette, etc.) renforcent la sécurité des paiements sur internet. Le système CB dispose d'une base de données alimentées en permanence : le Système d'Information Cartes Bancaires (SICB).
La mise en œuvre en Europe des spécifications EMV* (Europay, Mastercard, Visa) pour la carte à puce représente un enjeu majeur dans la lutte contre la fraude transfrontalière. Elle concerne non seulement les cartes elles-mêmes, mais aussi leurs dispositifs d'acceptation (terminaux, automates de paiement et de retrait) qu'il convient de migrer vers les nouvelles spécifications pour pouvoir bénéficier d'un niveau de protection égal partout en Europe. Les banques européennes s'étaient engagées à achever cette migration pour fin décembre 2010, et malgré un léger retard, cet objectif est sur le point d'être atteint.
La course technologique contre les cyberfraudeurs se gagnera aussi en mettant en place une traçabilité des flux financiers criminels en développant les collaborations européennes institutionnelles et scientifiques.
La Convention sur la cybercriminalité de Budapest du 21 novembre 2001 constitue aujourd'hui le texte de référence en matière de coopération internationale dans la lutte contre la cybercriminalité. L'union vient aussi de se doter d'un nouveau Centre européen de lutte contre la cybercriminalité (EC3). Sa mission consiste à cartographier et à suivre les sources de cyberattaques à l'extérieur de l'UE. Il a pour vocation d'apporter son expertise aux enquêtes de police et de coordonner les informations, mais n'a pas pour mission d'élucider les crimes à la place des polices nationales.

B5 - E-réputation : quels risques pour les entreprises et les particuliers ?

Intervenants :

- Nicolas KATZ : Consultant en stratégie et médias sociaux, Blufluence,
- Jean-Paul PINTE : Spécialiste en management et en veille stratégique des risques cybercriminels, docteur en Information Scientifique et Technique, Maître de conférences, Université Catholique de Lille,
- Hugo SALDMANN : Avocat spécialiste en Droit pénal et Cybercriminalité, Cabinet Saldmann,
- Isabelle CAMBRELENG : Directrice des activités Internet et des médias sociaux, Groupe la Poste,
- Albéric GUIGOU : Président et Co-fondateur, Réputation Squad.

Résumé des interventions :

Les médias sociaux ou les réseaux sociaux sont devenus des éléments moteurs du développement des entreprises françaises au niveau national et international. Cette révolution des espaces industriels se fait par la collaboration croissante des employés des entreprises. La fragile frontière entre vie publique et vie privée, au sein de l'entreprise, nécessite de nouvelles règles de gestion des ressources humaines qui impliquent chaque niveau de l'entreprise dans une logique transversale et non plus horizontale. La réussite de l'intégration aux réseaux sociaux passe par une éducation pertinente à l'e-réputation.
Il n'existe pas de droit à l'oubli sur les réseaux sociaux. L'indélébilité des comptes génère une ADN numérique et une cartographie individuelle numérique qui impactent chaque internaute. En l'absence d'un code de l'internet ou d'un code des médias sociaux, les juges cherchent dans l'arsenal juridique les textes susceptibles d'êtres appliqués pour traiter les différents niveaux d'attaque à la réputation individuelle ou commerciale. Mais ce n'est pas le droit qui façonne les actions menées sur internet, c'est l'internet qui façonne le droit. Une réflexion est menée dans ce sens par le Sénat..

I. Les problématiques

Les médias sociaux sont largement utilisés par les individus et les entreprises en qui sous-estiment les risques potentiels en termes d'e-réputation. Les incidences à court terme et à long terme sur l'identité des acteurs sont peu prises en compte ou acceptées. Alors que les notions mêmes de fichiers et de protection des données personnelles font à juste titre débat, les individus et les acteurs économiques s'exposent de façon démultipliée sur la toile. Il n'existe pas de définition juridique de l'e-réputation, de son contenu, de ses contours et de ses limites. Il est seulement possible de conceptualiser ce qu'elle peut-être et d'en déduire comment elle peut être atteinte. Un cadre juridique se construit. Les enjeux de l'e-réputation relèvent de la protection de l'identité numérique individuelle.

L'ergonomie des réseaux sociaux, de nouvelles pratiques de communications individuelles, l'enjeu économique pour les entreprises sont autant de facteurs qui favorisent la confusion des espaces personnels et professionnels. Pourtant, ces deux aires de communication nécessitent des niveaux de vigilance et des règles différents. Les process de recherche sur la toile favorisent des cartographies individuelles et collectives qui impactent l'identité de chaque internaute. Les moteurs de recherche pré-paramétrés peuvent générer des informations faussées ou même des diffamations. Il n'existe pas de droit à l'oubli sur les réseaux sociaux. En effet, le nettoyage des bases est impossible. L'indélébilité des comptes créés est à l'origine d'une ADN numérique. Malgré des avances jurisprudentielles, un véritable droit à l'oubli de l'internaute reste à construire.

Les entreprises doivent évoluer avec ces outils médiatiques qui impactent leur devenir et leur activité opérationnelle. L'enjeu est d'abord économique, une entreprise qui n'est pas présente sur les médias sociaux ou qui n'utilisent pas les bons outils de communication sur ces médias réduit d'autant sa visibilité et sa fiabilité pour ses interlocuteurs. Les entreprises françaises ne peuvent pas ignorer ce vecteur de la communication dans leur stratégie commerciale. Les réseaux sociaux offrent aux entreprises, quelle que soit leur taille, une visibilité et une valorisation sur le marché national et international. Les média-sociaux sont des caisses de résonance pour les entreprises et les retombées maitrisées seront profitables aussi aux collaborateurs. Pour celles qui développent cet outil auprès de leurs collaborateurs, ce sont les lois de la gravité managériale qui sont à revisiter en cas de crise mais aussi sur les modes décisionnels.

II. Les solutions

Le droit français ne connait pas de spécificités particulières au domaine virtuel et au droit de l'Internet. En absence d'un code de l'internet ou d'un code des médias-sociaux, les juges puisent dans l'arsenal juridique les textes susceptibles d'êtres appliqués. Les atteintes à l'e-réputation recouvrent les notions de diffamation, d'injure pour les personnes et de dénigrement pour les entreprises. L'atteinte à la vie privée se heurte à l'écueil de l'exposition volontaire des personnes sur les réseaux sociaux de parties de leur vie privée. L'usurpation de l'identité numérique, c'est à dire tous les éléments qui peuvent être rattachés à une personne permettant son identification, définie dans la loi d'orientation et de programmation pour la performance de la sécurité intérieure (15 mars 2011), commence à donner ses premiers résultats judiciaires. Les entreprises en cas de publicité trompeuse ou

agressive peuvent se tourner vers les juridictions pénales ou commerciales.
En règle générale, la justice peut-être efficace pour faire cesser les troubles causés par l'atteinte à l'e-réputation et, d'autre part, obtenir réparation du préjudice. Mais la définition de la personne responsable n'est pas toujours évidente. Il y a aussi une réelle difficulté à voir appliquer le droit sur un territoire quasiment infini qu'est celui d'internet. Mais la nécessité de centraliser et de rationaliser les comportements sur internet se fait de façon plus prégnante. Les jurisprudences donnent un contour à la notion de l'e-réputation. Mais il reste à formuler un véritable droit à l'oubli au profit de l'internaute.
Les managers doivent inverser la notion de risque car les atteintes à l'e-réputation ne sont pas une fatalité si l'introduction sur les médias-sociaux est menée au sein des entreprises avec tous les interlocuteurs dans un dialogue qui rapproche les interventions des utilisateurs. Il en résulte aussi une plus-value dans la production. Au sein de l'entreprise il faut sensibiliser pour sécuriser en expliquant et en impliquant les collaborateurs à l'image de l'entreprise. Les médias-sociaux intègrent chacun des collaborateurs dans une synergie commune. La protection de l'e-réputation par la prise de conscience des notions de sécurité et de cybercriminalité participe de cette même synergie.
L'exposition aux réseaux sociaux ne peut se contenter d'une transparence des activités de l'entreprise, mais doit s'accompagner d'une stratégie sémantique, c'est à dire la création du contenu efficace. Le recrutement de personnes capables de tenir la veille et la visibilité de l'e-réputation de l'entreprise est un élément important. La veille de l'e-réputation revisite les règles des ressources humaines en justifiant des opérations transversales entre différentes fonctions au sein de l'entreprise afin d'englober tous les enjeux, la finalité, les besoins et les risques. Les services de sécurité informatique ne sont pas les seuls interlocuteurs lors de cette phase de mise en confiance numérique avec les partenaires qui vont intervenir sur le réseau avec une porosité entre la sphère de l'entreprise et la sphère privée. C'est l'ensemble du maillage informatique et des acteurs au sein de l'entreprise et de leur vie privée qui sont impliqués.

B6 - Nouvelles technologies, nouveaux usages, nouveaux risques.

Intervenants :

- Michel PICOT : Journaliste, BFM Business,
- Dominique BOURRA : Directeur Nano JV,
- Pierre CALAIS : Membre du directoire NETASQ, vice-président Ingénierie et Opérations, président de l'association R&D-SSI,
- Aurélien FRANCILLON : Professeur sécurité informatique et des réseaux, EURECOM,
- Chekib GHARBI : Président-directeur général EuraRFID ,
- Alban SCHMUTZ : Senior VP business Development & Public Affairs, groupe OVH.

Résumé des interventions :

Internet des objets, informatique ubiquitaire, nanotechnologies, web 3 voir 4.0 : autant d'innovations en cours d'adoption ou bientôt adoptées qui élargissent le champ des possibles en matière de cybercriminalité. Quels sont les risques face à ces nouvelles technologies et surtout aux nouveaux usages qui en découlent et les prospectives associées à ce sujet ?

I. Les nouveaux risques

Le développement de technologies ou d'outils nouveaux est porteur de risques non identifiés au départ. C'est le cas de l'internet mobile ou du monde des objets interconnectés.
L'application d'une technologie à un système préexistant peut engendrer des failles de sécurité.
Le développement des technologies sans contact et l'implantation de puces RFID[1] sur des cartes de paiement pose des problèmes de sécurité des données. L'information des victimes potentielles est faible. Elles bénéficient de passeports à lecture optique, de cartes bancaires avec puce RFID dont les données sont lisibles à distance sans qu'elles le sachent. Elles ne bénéficient pas des systèmes de protection d'un réseau. Un opérateur averti, en moins de deux mois, peut réaliser un programme pour capter les données de ces documents. A titre d'exemple, l'association d'un système d'identification et d'une technologie sans contact permet aujourd'hui de démarrer une voiture en gardant la clef dans sa poche. La possibilité que les données permettant le démarrage à distance de la voiture soient piratées doit être prise en compte.
La technologie du « *cloud* » implique quatre exigences de sécurité : la disponibilité des données, leur intégrité, la garantie de confidentialité et la protection juridique. Des procédures de sécurisation des infrastructures peuvent être mises en place mais elles seront fragilisées par le mauvais comportement des clients. Dans 9

1 - RFID, radio frequency identification, est une méthode pour mémoriser et récupérer des données à distance.).

cas sur 10, une erreur humaine est à l'origine d'un incident de sécurité.
On ne doit pas confondre un exploit « *Zero-Day*[2] » et une attaque de type « *Stuxnet*[3] » qui comporte le vol pur et simple de deux certificats de sécurité. Cet exemple démontre que la protection « *physique* » des certificats de sécurité est insuffisante, ce qui pose un problème de préservation de l'intégrité de l'architecture du réseau et des données.

2 - ZERO DAY, est un exploit qui utilise une faille jusqu'ici méconnue du public. Un exploit 0 day est susceptible d'engendrer la création d'un ver car, par définition, la grande majorité des utilisateurs ne sera pas protégée contre cette faille jusqu'à ce qu'elle soit découverte et corrigée.
3 - STUXNET, est un ver informatique supposé développé conjointement par les États-Unis et Israël pour s'attaquer à des systèmes iraniens.

II. Les solutions

Une formation est nécessaire. Il faut sensibiliser les utilisateurs aux dangers d'une pièce jointe, au contrôle d'une clef USB ou d'une application téléchargée. Les entreprises doivent mener une réflexion en matière de sécurité. Il faut accompagner les évolutions, définir une charte de comportement, édicter des règles, informer les salariés. Il faut les mettre au cœur de la sécurité des risques et les rendre receptifs à leur responsabilité juridique. Les entreprises doivent, faire un choix concernant la dotation en matériels productifs : autoriser les salariés à travailler avec leur matériel privé (BYOD[4]) ou bien leur imposer un matériel configuré par l'entreprise et les autoriser à l'utiliser à des fins personnels (COPE[5]).
La sécurité globalisée doit être pensée et intégrée dès la conception de l'architecture matérielle des réseaux. Le cadre réglementaire fixant la certification des produits et les relations avec les fournisseurs ne doit pas être négligé.

4 - BYOD (bring your own device), Apportez vos appareils personnels.
5 - COPE (corporate owned personnally enabled), qui consiste à autoriser un usage personnel avec des terminaux fournis et gérés par l'entreprise.

La France a développé des compétences remarquables en cryptographie, technique visant à rendre un message inintelligible sauf habilitation. Toutefois, le vol des certificats qui a permis de débuter l'attaque «Stuxnet[6] » semble démontrer que la cryptographie n'est pas suffisante pour garantir la sécurité des données et des systèmes. Quelques pays, notamment Israël, développent des solutions innovantes en matière de biométrie. Par contre, dans ce domaine, la protection des droits individuels peut être contradictoire au regard de solutions de sécurité et créer des vulnérabilités. Les technologies de rupture dans le domaine de la sécurité nécessitent un décloisonnement des disciplines en matière d'innovation. Alors que, dans les laboratoires, aucune hiérarchie n'est imposée dans la phase de développement, et que beaucoup de latitude et de moyens sont accordés aux équipes, les Etats-Unis promeuvent le co-développement et l'interdisciplinarité. Un programme militaire très performant sur le cybergénome, analyse de virus servant à identifier la source de tout matériel électronique, se conjugue avec ceux de la DARPA (Defense advanced research projects agency) qui croisent les recherches cybernétiques et biologiques : cyber-anthropologie, cyber-génétique, cybersociologie, etc. Leurs laboratoires commencent à développer des composants électroniques créés à partir de protéines ou à utiliser de l'ADN synthétique pour stocker des données. En matière de brevets, les Américains conservent le leadership. Vient ensuite l'Europe, où les Allemands déposent la moitié des brevets, puis l'Asie au sein de laquelle le Japon a la prééminence.
Une solution consiste dans le recours à des hackers privés ou étatiques. Ils sont incités par le versement de primes à participer au renfor-

6 - STUXNET, c'est un ver qui espionne et reprogramme des systèmes SCADA commandant des procédés industriels.

cement de la sécurité. Des sociétés de hackers repèrent les failles de sécurité puis les commercialisent. L'agence de sécurité américaine organise des concours chaque année afin de recruter des hackers. « *Outsourcer*[7] » la sécurité peut aussi avoir un effet néfaste et réduire le niveau de vigilance de l'entreprise. Certains hackers identifient les failles mais n'informent pas les entreprises concernées. Ils vendent les informations à des cyberdélinquants, à des organisations criminelles, des États qui rémunèrent mieux que les entreprises ou les acteurs institutionnels.

7 - Outsourcer, confier une tâche à une société extérieure au lieu de la faire soi-même

B7 - Santé et cybersécurité

Intervenants :

- Béatrice BERARD : Responsable Système, C.H.U. de NANCY,
- Pierre AUBRY : Responsable pôle administrations et collectivités, Imprimerie Nationale,
- Eric GROSPEILLER : Fonctionnaire de Sécurité des Systèmes d'Information, Ministères des affaires sociales,
- Jean-François PARGUET : Directeur du pôle Technique et Sécurité, Responsable sécurité des Systèmes d'Information, ASIP Santé,
- Yves BEAUCHAM : Chargé de mission Systèmes d'Information de l'offre de soins, Agence Régionale de Santé Nord-Pas-de-Calais.

Résumé des interventions :

Le secteur de la santé n'échappe pas à la cybercriminalité. La présence de RSSI dans les hôpitaux est désormais une nécessité justifiée par la dématérialisation du système de soin, les échanges électroniques entre les professionnels de santé et les grandes réformes de la santé (le dossier médical personnel informatisé 2004, la télémédecine 2009, l'hôpital 2012). La sécurité numérique du secteur de santé se développe, notamment par le biais

I. La santé n'échappe pas à la cybercriminalité

En France, la loi « *Hôpital, patients, santé et territoires* », du 21 juillet 2009, vise à améliorer l'offre de soin par le développement des technologies numériques. Un responsable doit animer et coordonner la sécurité. Si la sécurité est assurée (confidentialité), il existe parfois une absence d'intégrité et de disponibilité pour accéder au dossier des patients. En effet, le même réseau transporte les données destinées à l'administration et les offres de services aux patients. Ces risques potentiels peuvent par exemple conduire à un retard des commandes de médicaments.
Des attaques sont susceptibles de peser sur la vie humaine des patients. Des attaques virales peuvent porter atteinte aux fichiers administratifs de gestion des admissions. En outre, les industriels développent des produits sans placer la sécurité ou cœur des instruments. Par exemple, il n'existe pas de règles en la matière, bien qu'une pompe à insuline ou un pacemaker actionnable à distance devraient faire l'objet d'une sécurité intégrée. En 2009, un vers a touché des milliers de systèmes d'information et certains hôpitaux ont été infectés par le biais de clés USB.
Les menaces sont le plus souvent internes à l'établissement. Les données des patients et les données personnelles représentent une valeur marchande pour les organisations criminelles. Lors de la pandémie H1N1, on a pu noter sur le web des campagnes de spams pour un médicament "*Taniflux*"qui était une contrefaçon.

II. Une sécurité numérique en développement

Pour faire face aux risques numériques, il existe l'Agence des systèmes d'information partagés (ASIP). Il n'est pas envisagé un CERT santé qui nécessiterait des moyens énormes. En revanche, il existe une synergie entre le CERTA et l'ANSSI.
Le programme « *Hôpital numérique* » a été une première fois évoqué en 2008, mais il a véritablement débuté en 2012. La sécurité des soins est une priorité permanente qui intègre la confidentialité sur la santé du patient et la sécurité des systèmes d'information pour la production des soins. Avec le plan « *Hôpital public 2012* », 35 établissements de la région Nord pas de Calais se sont unis pour mettre en œuvre une politique de sécurité avec le déploiement d'instruments pour assurer la confidentialité, la continuité de l'activité et un socle de travail commun. Ce regroupement, qui concerne à la fois les hôpitaux et les cliniques au plan local voire régional, permet des résultats positifs. Le retour d'expériences est capitalisé par des livrables mis à la disposition des services qui n'ont pas franchi le pas.
L'exemple du CHU de Nancy peut être souligné. Le principe de l'hôpital numérique repose sur une mutualisation de l'action des établissements dans différentes filières au nombre de 15 (linge, technologie de l'information et de la communication, etc) en améliorant la fonction d'achat et en faisant partager les bonnes pratiques. Le principe repose sur la mutualisation des connaissances et des appels d'offre. Ainsi, dans le domaine de la sécurité des systèmes d'information, il est proposé une démarche structurée reposant sur une politique de sécurité déclinée, des authentifications fortes, l'organisation de la sécurité en interne à l'établissement (maitrise d'ouvrage, agrément des hébergeurs), une politique de gestion de traces, la mise en place de signatures électroniques, la mise en œuvre d'un annuaire et d'habilitations, l'installation de sécurité logique comme la carte d'établissement. Naturellement, l'ensemble des obligations doit être décliné dans chaque établissement.
L'agence des systèmes d'information partagés de santé favorise la dématérialisation des données de santé en prenant en compte la gestion du personnel de santé (22 professions réglementées). Sur le plan structurel, elle produit les 850.000 cartes de santé du personnel, assure la sécurité de la messagerie sécurisée de santé et le dossier médical « personnel ». Sur le plan du référentiel et de l'interopérabilité elle gère les 600 pages de spécifications permettant de travailler selon les normes établies, le fichier des identifiants nationaux de santé, donne l'agrément pour les hébergeurs de données de santé et délivre l'accréditation de conformité aux textes des produits des industriels. Parmi les contraintes, on relèvera que le processus protégeant l'hébergement des données personnelles de santé ne garantit pas en revanche, faute d'un document spécifique, les données de santé. En ce qui concerne l'externalisation de ces données, on constatera que la directive service ouvre les appels d'offre à tous les prestataires européens. Enfin, avec le « *Cloud* » on est dans l'impossibilité de situer la donnée dans l'espace et de dire s'il relève d'une gestion privée ou publique.
L'imprimerie nationale, tiers de confiance, assure l'impression des titres régaliens sensibles sécurisés (carte d'identité professionnelle numérique). Elle met en œuvre le référentiel général de la sécurité, gère et héberge les moyens de cryptologie. Le centre des professionnels de santé assure la certification de l'identité numérique et la protection contre les usurpations d'identité. Mais, avec

l'augmentation du volume de données personnelles de santé échangées (Ex : IRM, scanner), il existe une menace d'action des cybercriminels. L'imputation, la traçabilité, l'intégrité sont des mesures fortes et les moyens de sécurité doivent être toujours à jour. Le service doit permettre une utilisation simple des moyens à l'instar d'une carte bancaire avec un minimum d'interruption et une possibilité de révocation immédiate 24 h/24, 7 jours/7.

B8 - Regard croisés sur les stratégies de cyberdéfense

Intervenants :

- Lieutenant-colonel Patrice TROMPARENT, Délégation aux affaires stratégiques,
- Arnaud COUSTILLIERE : officier général cyberdéfense,EMA,
- Rob SMEATON : Wing Commander,SEAE,
- Wolfgang ROEHRIG : Project Officer Cyber Defence,EDA,
- Lieutenant-général (ret) Johannes KERT : ancien chef d'état major des armées estoniennes.

Résumé des interventions :

Les états sont désormais nombreux à affiner les stratégies de cyberdéfense. Des alliances sont en place d'autres assument leur cyberpuissance.
L'atelier s'est attaché à relater les stratégies de cyberdéfense, leur efficacité, les améliorations possibles qui passent par une meilleure interopérabilité étatique.
Par ailleurs, l'importance exacerbée de la formation se voit confortée par les nouveaux dispositifs d'enseignement générés que confortent la présence et l'importance des réservistes et autres volontaires dans la cyberdéfense.

I. Le Consensus

Dans le concert européen les domaines liés à la cyberdéfense sont multiples et le « *safe and secure* » est devenu une préoccupation constante. Le service de défense de l'UE s'est dès lors attaché à coordonner les efforts de chaque pays membre en vue de limiter la dispersion, à développer des ressources pour le cyberespace au sein de l'UE et à sensibiliser à l'enjeu du cyberespace européen.
En raison de la porosité des armées avec les opérateurs privés, en particulier dans le cadre des missions civiles largement privilégiées par l'UE, l'axe d'effort a été celui des échanges entre les pays et la création de telles opportunités.
In fine, c'est la notion de confiance à générer qui sous-tend toute action et l'échange de renseignements entre les pays.
En résumé, résilience et protection des équipements, développement de capacités communes, échanges d'informations et « *process* » en cohérence sont autant de vecteurs d'actions porteurs de l'efficacité recherchée.
L'Europe, en tout état de cause, affirme le principe de la séparation stricte entre militaire et civil et veut garantir l'observation des traditions nationales en matière de cybersécurité.

II. Des solutions

Si la France érige en priorité une stratégie industrielle « *cyber* » sous la gouvernance et l'autorité du Premier ministre par le biais de l'ANSSI, elle ne mésestime pas la toile et son caractère primordial dans le nouvel espace de combat, le cyberespace.
Depuis mai 2011, de nouvelles mesures ont été prises visant à garantir la cohérence des ordres, la vigilance sur internet et la préparation des forces à l'éventualité de telles attaques.
Par ailleurs, l'accent est porté sur la formation avec l'instauration de modules de formations à l'école des transmissions de Rennes, à l'ESM St Cyr, à l'ENSTA, chez Suptelecom et à l'université Bretagne sud avec la création de l'ENSIBS[1].
Enfin une réserve citoyenne de volontaires vient ouvrir le volant des ressources humaines affectées à cet effort.

1 - L'École Nationale Supérieure d'Ingénieurs de Bretagne Sud (ENSIBS) est une école d'ingénieurs agréée par la CTI dépendant de l'Université de Bretagne Sud.

L'attaque « *cyber* » de 2007, en Estonie, a fait prendre conscience, non seulement par ce pays, mais par toute l'Europe, de la vulnérabilité des réseaux numériques d'état. Située à la frontière de l'est et de l'ouest du « *vieux continent* », l'Estonie a été désigné par l'OTAN pour y implanter la coopérative Cyber Défense Center of Excellence (CCDCOE).
Dès 2009, ce pays a constitué, sur la base du volontariat, une ressource humaine, composée de spécialistes en IT, en sciences juridiques, ainsi que des analystes (l'Estonian Defence league, dont la philosophie pourrait utilement se prêter à duplication dans d'autres états).
Les tâches principales de ce dispositif résident en des manonœuvres et exercices , comme de nouveaux tests d'intrusion dans les systèmes.

Au global les solutions les plus idoines apparaissent être l'instauration de synergies entre les structures adoptées, la préparation des personnels (formation) et une coopération optimisée entre les Etats (Européens en premier lieu).

B9 - Développement informatique sécurisé

Intervenants :

- Bertrand GARE : Informaticien.
- Eric FILIOL : Directeur R&D, laboratoire de virologie et cryptologie opérationnelle, ESIA,
- Bernard ROUSSELY : Responsable commercial SSI, Bertin technologies,
- Vincent BUFFRERNE : Expert sécurité, SOGETI,
- Franck ERMEL : Ingénieur principal des études et armements, DGA, Ministère de la défense.
- Martine GUIGNARD : Responsable sécurité des systèmes d'information, Imprimerie nationale.

Résumé des interventions :

La dimension de la sécurité du code est stragégique, industrielle et humaine. Elle requiert une formation spécifique en amont associée à une forte senbilisation du développeur. Le développement sécurisé ne peut reposer sur la seule responsabilité du développeur. La qualité de la prescription en matière de cahier des charges, d'architecture du produit et d'intégration de la SSi dans les coûts est facteur d'efficacité et d'économies. La formation continue du développeur, un tutoring et un intéressement à son environnement limitent les productions de codes vulnérables.

I. Un environnement stratégique

La vulnérabilité du code a une dimension critique et stratégique. Elle s'applique aux industriels dont la R&D est stratégique dans une vision économique globale, l'objectif final étant le monopole du code d'un produit mondialisé. L'outillage des codes devrait être une des préoccupations de la R&D européenne. On ne peut demander aux prescripteurs et aux développeurs de maîtriser toutes les évolutions rapides de langages, de codes et des standards sans outils concurrentiels adaptés.

La responsabilité est essentiellement celle du prescripteur. Il doit définir un environnement normé et décliné sur toute la gestion du projet comportant les règles de codage, d'organisation et de principes architecturaux. Il doit séparer la partie « *intégration-qualification* » du « développement» afin d'obtenir une diversité d'outils spécifiques de contrôle de la qualité du code. Il faut élargir l'approche des outils SSI par une prise en compte précoce, globale et encadrante des marchés sensibles. Outre les prescriptions techniques qui créent un contexte de confiance on peut y inclure un régime d'habilitation au

marché de personnes morales et des habilitations individuelles.
L'approche de sécurité doit être intégrée au plus tôt pour diminuer les coûts, provoquer une adhésion des acteurs de toute la chaîne de production et, par conséquence, provoquer un développement meilleur. La SSI intègrera à cet effet les systèmes d'information, des matériels et des logiciels. La première préoccupation d'une architecture est celle de la validation des algorithmes, du cryptage et de l'implémentation logicielle. Les principes d'architecture classique peuvent être regroupés sous un concept américain, le TCB (trusting computing base). Il doit prendre en compte l'impact de failles logicielles spécifiques, car beaucoup d'attaques sur des d'applications brisent les défenses de systèmes entiers, ce qui est inacceptable.
Il faut choisir des outils ayant une capacité d'évolution et d'enrichissement en fonction de la compréhension des problèmes. Il existe en « *open source* » des outils améliorables et paramétrables qui permettent d'éviter des outils propriétaires très couteux. Enfin, on peut préciser que le prescripteur peut s'appuyer sur des guides de l'ANSII ou du CERTA pour rédiger son cahier des charges et son analyse du risque. Il peut également consulter le code des marchés publics, art 180 al 5, qui comporte la mention d'éditeurs fiables.
Les logiciels achetés comprennent des composants étrangers de programmation. Leur profusion et leur origine ne permettent pas de vérifier la qualité de leur code. Le problème est aigu pour les automates dont la sécurité n'est pas la fonction première. Le traitement des hôpitaux français montre une architecture reposant sur l'intégration de produits standards et de SCADA mal programmés et sans analyse de risque. La modification des programmes implique une perte de l'agrément de santé. Les démonstrations de piratage de matériels médicaux, pacemakers compris, montrent les faiblesses de l'assemblage de framework sans test significatif. On doit relever l'importance du cahier des charges. En matière de machines de production, il convient d'examiner l'ajout de codes corrigés aux codes initiaux livrés avec la machine. Il est difficilement acceptable que des applications intéressant des infrastructures de sécurité et de transport vitales pour les systèmes et les personnes n'impliquent pas, en cas de déficience de sécurité, une incrimination civile et pénale significative. Il faudra que les éditeurs aient des comptes à rendre. Techniquement, on peut comprendre un « *zéro day* » mais on ne peut tolérer la mise sur le marché de produits non terminés, testés sur des simples règles commerciales et impliquant la fourniture d'une centaine de patches par ans sur certains produits qui deviennent non maintenables. Cette démarche doit inclure les assureurs et reposer sur une responsabilité vis à vis du citoyen pour les systèmes critiques et un respect des certifications.

II. L'accompagnement managérial du développeur

Les écoles d'ingénieurs devraient intégrer, même si cela doit relever d'une prescription étatique, 15 à 20 heures consacrées à l'étude de la sécurisation des codes afin de les intégrer dans une forte logique. Elles prôneraient le choix de codes « *propres* » avec des tests récurrents mettant en valeur les conséquences des erreurs de programmation. Cette interactivité impliquerait une forte réceptivité des étudiants, notamment si on y intègre des formations offensives et défensives.
Il faut également mettre en place une mise à niveau régulière des chefs de projets et des

développeurs en intégrant le fait que la production de code sécurisé a une dimension économique. Cela est toutefois plus difficile pour les systèmes embarqués, aux ressources plus faibles, qui posent un problème de transposition. C'est un nouveau challenge en matière de R&D dans des contraintes de coûts acceptables.
Le chef de projet n'a pas vocation à se substituer au développeur. Il doit vérifier si ce qui est mis en production est correct. Cela nécessite un travail de démonstration des conséquences du bug. L'audit du packaging permet d'élever les privilèges, les contrôles sur la plate-forme de production et de fortement tester la production. Il importe d'engager un travail de certification et de mise à niveau des formations des développeurs. Il convient également de mettre en place la définition de règles de codage, même en s'inspirant de standards. L'ANSII a émis un CERTA et publié des notes d'informations relatives au développement sécurisé des applications Web et clonées. Les éditeurs maintiennent le produit un certain temps, mais il est difficile de suivre les évolutions du produit. Le CERTA relève les systèmes, logiciels répandus et les SGBD ainsi que leurs correctifs sur un seul document dans une vision panoramique des produits supportés. Il émet un bulletin d'accompagnement d'actualité qui attire l'attention sur des applicatifs centraux bien développés, mais qui peuvent se voir affectés de modules complémentaires pas toujours bien maintenus en SSI.

B10 - La résilience internet

Intervenants :

- Jean-Luc LEFEBVRE : Colonel , IRSEM ,
- Stéphane BORTZMEYER : Ingénieur R&D, AFNIC,
- François CONTAT : Inspecteur ANSSI , spécialiste des réseaux,
- David SIMPLOT RYL : Directeur du Centre de Recherche, INRIA Lille Nord Europe,
- Guillaume VALADON : Inspecteur ANSSI , spécialiste des réseaux.

Résumé des interventions :

Des moyens de plus en plus précis existent désormais pour définir et mesurer le résilience de l'Internet. Parfois simples, ils permettent de prévenir des dommages de grande ampleur. A ce jour, une panne généralisée de tout l'Internet ne semble pas envisageable, d'autant plus que l'action d'un seul acteur hostile ne peut pas avoir des conséquences importantes.

I. Un champ sémantique large

A ce jour, il n'existe pas encore de définition officielle de la résilience. Ce terme s'applique à l'environnement, la physique, aux sciences humaines et sociales ainsi qu'à la défense et à la sécurité nationales. Il est important de souligner que la notion de résilience ne relève pas seulement de la technique, mais également d'une dimension sociétale et sociale.
Une première approche repose sur la considération d'un système complexe, résistant à un certain nombre d'attaques (attaques aveugles mais aussi des pannes délibérées) et qui a la capacité de les absorber sans se départir de ses fonctionnalités principales, et de redémarrer. On peut en dégager un concept de « *robustesse* » de l'architecture.
La résilience est liée avant tout à celle d'êtres humains qui réfléchissent, coopèrent, trouvent des solutions et les exploitent. Dans toutes les grandes pannes de l'internet, le rétablissement fonctionnel est le fruit de décisions prises collectivement.
De manière plus générale, on peut considérer la résilience d'internet comme le résultat de l'action conjuguée de nombreux acteurs avec plusieurs opérateurs et exercée dans le contexte de plusieurs infrastructures interconnectées entre elles dans un maillage dense et complexe.

II. Des solutions

Un questionnement vise les pistes à explorer pour hausser le seuil de résilience d'une configuration informatique : un recensement exhaustif des menaces possibles sur internet, la mesure des risques encourus face à une volonté de nuire d'un individu isolé, voire d'une organisation mafieuse qui voudrait perturber gravement internet. Il en est de même pour un état qui voudrait mener une attaque ciblée vers un autre état. On doit également s'interroger sur la définition de règles simples à respecter pour sécuriser

et renforcer un réseau. A l'instar du vivant, certains chercheurs prônent une amélioration de la résilience par le jeu d'une « *diversité génétique* » en utilisant des logiciels de conception différente.

Il existe une grande différence entre la perturbation d'internet, action relativement facile à accomplir, et l'arrêt d'internet, de manière générale et sur une longue période, qui est très difficile. Techniquement une menace représentée par un état, via une agence étatique spécialisée, reste possible notamment si celle-ci dispose de moyens et de capacités techniques ou humaines. Une action hostile vis à vis de la France serait très compliquée, le maillage étant très fort avec ceux qui partagent nos frontières. Reste que le « *plantage* » d'une partie d'internet est possible et que cette menace est à prendre en compte. Le fait de prendre conscience des risques est déjà une manière de s'y préparer et permet de mieux se protéger. Il est également important d'aborder l'aspect « physique » de l'internet à l'instar du risque engendré par une grande concentration sur un même lieu de moyens informatiques (opérateurs et acteurs internet dans le même centre d'hébergement).

Pour mesurer la résilience d'internet, une solution consisterait à « *casser des éléments* », à l'instar de ce qui se pratique en résistance des matériaux. Cette solution n'est pas possible compte-tenu des enjeux économiques pour les entreprises. Il est donc nécessaire de mesurer la résilience sans faire d'ingérence, en se focalisant sur deux protocoles d'internet que sont BGP (Border Gateway Protocol) et DNS (Domain Name System), éléments structurels d'internet qui servent à le construire et qui permettent son fonctionnement.

L'Observatoire de la résilience de l'internet cherche avant tout à scruter ce qui se passe sur l'internet français, sachant que les différentes données sont souvent analysées par des agences américaines. Il recense l'utilisation des bonnes pratiques, quitte à en proposer de nouvelles. La démarche de l'Observatoire nécessite plusieurs étapes : définir les indicateurs pour faire des mesures, puis trouver des sources d'information pour alimenter ces indicateurs et mesurer ces derniers en utilisant avant tout des sources publiques, en utilisant le réseau RIPE (Réseaux IP Européens). Il faut, enfin, faire les mesures et interpréter les résultats pour déterminer le coût de la résilience. On peut donc tout à fait mesurer cette résilience à condition d'être à l'écoute et de veiller en permanence de l'évolution du réseau.

Des règles simples comme le durcissement d'un réseau ainsi que les soins à apporter à la configuration de cloisonnement permettraient de réduire les risques. Beaucoup de règles existent mais ne sont pas appliquées. Les comportements et les règles de bon sens ont leur importance, comme d'ailleurs une politique de sécurité interne. Les mesures propres à la résilience informatique sont connues des spécialistes et ne sont pas forcement propres à internet. Si elles ne sont pas parfaitement appliquées, c'est par ignorance, mais aussi parce qu'elles entrainent un coût .

La « *diversité génétique* » est une bonne chose, comme faire appel à plusieurs constructeurs et équipementiers, mais cette diversité entraîne des coûts (négociations moindres, formation, ressource humaine maitrise, risque dans la configuration du réseau).

B11 - Monétique et commerce en ligne

Intervenants :

- Laurent PENOU : Lyra Network,
- Nathalie FEYT : responsable de l'activité Evaluation THALES,
- Benjamin MARECHAL : expert en moyens de paiement scripturaux Banque de France,
- David NACCACHE : cryptologue, master Université Paris 2,
- Patrick YVARS : commissaire de Police, chef de la Brigade des fraudes aux moyens de paiement BFMP.

Résumé des interventions :

Le commerce en ligne s'est largement développé au gré des nouvelles technologies. Les transactions qui passent par la toile doivent être sécurisées, car une faille dans le système entraîne des conséquences financières, des contentieux difficiles et une perte de confiance. La question de la maîtrise des risques liés à l'utilisation des cartes de paiement est alors clairement posée ainsi que celle de la construction d'une réponse aux menaces qui garantit la confiance du client.

I. Les problématiques

Le questionnement porte habituellement sur le vol d'une carte bancaire. En réalité, pour 99% des points de compromission, les dangers ne viennent pas du net mais du commerce «*de la vraie vie*». C'est-à-dire que le commerçant indélicat, qui reçoit un paiement par carte bancaire dans son établissement, va mettre en oeuvre des formules pour tenter de retenir le cryptogramme (les 3 chiffres qui se trouvent au dos de la carte). En effet, c'est la seule information non imprimée sur le ticket édité par le lecteur de carte. Il est rappelé que pour utiliser une carte, il faut 3 informations : le numéro de la carte, la date d'expiration et le cryptogramme.

La difficulté réside dans l'objectivation et la mobilisation d'une ressource humaine et technique pour analyser une « *suspicion de fraude* ». Aujourd'hui, on ne sait pas évaluer la fraude. Surtout, on ne sait pas empêcher la réutilisation des données récupérées à des prix insignifiants à partir de disques durs ou de téléphones mobiles vendus sur e-bay sans vidage préalable. Le rôle de l'Observatoire de sécurité des cartes de paiement est de surveiller les mouvements incohérents, répétitifs dans un espace déterminé et limité.

II. La construction d'une réponse aux menaces

Des préconisations peuvent être formulées. La première est de mettre en place une sécurité active qui passe par l'adaptation à l'évolution des menaces. Il convient de réaliser un « *journal* » des événements qui puisse permettre de comprendre les incidents, leur cinématique et le degré de menace. Dès qu'un point de compromission est identifié une course « *défense / attaque* » se met en place. En général, la défense est une réponse à l'attaque et les techniques et les parades utilisées pour la défense ne peuvent pas servir à la prévention, car elles sont dépassées par l'évolution technologique et la diligence des attaquants.
La seconde réside dans la construction d'une sécurité passive qui comporte des dispositifs automatiques de surveillance des réseaux. Les statistiques et les réseaux Bayesiens vont permettre de construire des algorithmes qui aident à déceler des attaques, les clonages de cartes en analysant l'évolution des statistiques des comportements.
Quelle que soit la nature de l'attaque, le commerçant doit anticiper la nature de la menace et mettre en place une sécurité préventive en recherchant ses vulnérabilités, en estimant leur probabilité de survenance et les coûts associés.
De sa réactivité résulte la mise en place d'une sécurité défensive efficace. Le problème majeur concerne le stockage des données et le vol d'identité. La sécurité défensive impose de ne pas conserver les numéros de carte et notamment les cryptogrammes.
Certains commerçants stockent les données. Il est possible de les identifier. Pour attirer la clientèle ils utilisent la technique du « *one click* » ou le paiement en « *trois fois sans frais* », ce qui atteste leur connaissance du client et le non respect du code monétaire et financier. De plus, on constate l'apparition de faux numéros.
Les clefs du succès pour limiter la fraude résultent de la réactivité des acteurs : l'acheteur, s'il prend rapidement conscience de l'usurpation de sa carte, fera intervenir sa banque qui réagira d'autant plus rapidement que l'opération n'a pas encore fait l'objet d'une compensation.
Le commerçant fera appel à une assurance s'il pressent une fraude concernant le paiement d'une commande.
Concernant les particuliers, la Fédération e-commerce et vente à distance (FEVAD) conseille de s'adresser à un liste d'opérateurs établis en France et membres d'une fédération professionnelle. La loi impose également au vendeur de diffuser sur son site ses coordonnées postales, électroniques ainsi que son numéro de téléphone et ses conditions de vente.

III. les attentes

La première est la constitution d'un ensemble de pratiques visant à empêcher la réutilisation des données et les vols d'identité.
Il importe de ne pas museler l'activité d'un groupe par une globalisation (analyse globale d'un système d'intérêt local) qui masquerait la complexité du phénomène et conduirait à des solutions non appropriées pour résoudre le problème posé. Trop de sécurité tue la sécurité.
Le commerce en ligne nécessite des moyens de paiement spécifiques pour assurer la sécurité et entretenir des relations de confiance. Il conviendra dans ce cadre de finaliser des protocoles de moyens sans contact (NFC) fiables.

B12 - Quelle politique de sécurité des systèmes d'information adopter en entreprise ?

Intervenants :

- Fortuné Barnard : consultant,
- Gil Delille : Directeur Sécurité des Systèmes d'Information, Groupe Crédit Agricole,
- Eric Dupuis : Responsable du pôle Sécurité, Orange Consulting,
- Didier Gras : Directeur Sécurité des Systèmes d'Information, Groupe BNP Paribas,
- Lazaro Pessachowicz : Président du CLUSIF, Responsable Sécurité des Systèmes d'Information, CNAMTS.

Résumé des interventions :

La politique de sécurité des systèmes d'information, qui s'intègre dans la politique de sécurité de l'entreprise, est un acte de management qui implique tous les acteurs, du dirigeant aux métiers. Elle doit conjuguer éléments stables – les principes – et éléments évolutifs – les technologies. En tout état de cause, il lui faut formaliser des objectifs précis et en assurer le suivi.

I. Les problématiques

La difficulté première consiste à définir la politique de sécurité des systèmes d'information, dans un contexte qui évolue très rapidement, en raison de la dématérialisation des activités, de cycles techniques de plus en plus courts, et de l'évolution des usages et de la « *professionnalisation* » de la cybercriminalité. Cette définition implique l'ensemble de l'entreprise, du dirigeant aux collaborateurs, le RSSI ne pouvant aller contre les métiers. Toutefois, le niveau d'exigence posé peut être en décalage avec la culture « *sécurité* » de l'entreprise, d'autant que la tentation est de couvrir tous les risques. Or le risque « *zéro* » n'existe pas.
La définition et la formalisation d'une politique de sécurité, aussi nécessaire qu'elle soit dans toutes les structures, pourrait ne concerner que les plus grandes entreprises. Toutefois, il est avancé que le dirigeant, quelle que soit la taille de son organisation, nourrit des inquiétudes sur la sécurité de son système informatique. C'est déjà un début de politique de sécurité.

II. Des solutions

La politique de sécurité des systèmes d'information en entreprise est un acte de management qui exige la définition d'objectifs clairs qui doivent

être partagés par les collaborateurs. Elle implique donc la gestion des ressources humaines. Cette exigence de clarté conduit la nécessité de la formaliser, ne serait-ce que « *pour mieux savoir où l'on veut aller* ».
Elle doit être révisée tous les 2 ou 3 ans. Il faut alors distinguer :
• une partie « *hors technologie* » qui demeure constante : quels sont les acteurs, les rôles, les enjeux ; on est ici dans la gouvernance du système d'information ;
• une partie qui apporte les solutions techniques.
A cet égard, il convient de souligner qu'on n'investit pas pour la sécurité. Le poste de travail évolue pour d'autres raisons que la sécurité qui doit en conséquence adapter ses règles. Ces évolutions doivent fournir l'opportunité de se rapprocher de la cible.
La politique de sécurité se déroule dans le temps, pour que l'entreprise gagne en « *maturité* ». La résolution d'une étape permet de passer à l'étape suivante. Le maillon faible étant « *l'humain* », il faut beaucoup de pédagogie. « *On ne fait de la sécurité pour la sécurité* ».
Il faut connaître les risques et définir le risque admissible. Les décideurs de l'entreprise doivent clairement indiquer leurs attentes en matière de sécurité. C'est aussi une contrainte budgétaire : chaque exigence de sécurité est un investissement, qui appelle à des arbitrages entre celles vers lesquelles faire porter les efforts et celles qui doivent appeler des simplifications.
D'une façon plus générale, la définition de la politique de sécurité des systèmes d'information passe par l'écoute des métiers. Être RSSI (Responsable de la Sécurité des Systèmes Informatiques), c'est exercer une fonction d'expert-ouvrage. Le RSSI ne s'oppose pas, il accompagne les métiers pour la maîtrise des risques.
Enfin, la politique de sécurité des systèmes d'information est un domaine qui se contrôle. Elle entre dans le champ du contrôle permanent, par la définition et le suivi d'indicateurs pertinents. Des audits externes sont un plus.

B13 - Quelle politique de sécurité pour le système d'information des collectivités territoriales ?

Intervenants :

- Maurice de BOSSCHER : responsable technique – Cre@tic,
- Rémy FEVRIER : Commandant (gendarmerie nationale), maître de conférence associé Université de Paris 1,
- Hervé FORTIN : Responsable de la Sécurité des Systèmes d'Information au Conseil général de l'Aisne,
- Thierry HENNIART : Responsable de la Sécurité des Systèmes d'Information au Conseil régional Nord pas-de-Calais,
- Michèle MARET : responsable du pôle SSI, déléguée de l'observatoire zonal SSI de la zone nord – ministère de l'intérieur.

Résumé des interventions :

Avec la dématérialisation, de nombreux processus (dont les appels d'offres) et le développement de l'administration électronique, le système d'information des collectivités territoriales s'est fortement complexifié et diversifié. Nous sommes face à une prise en compte très inégale de cette problématique suivant les collectivités territoriales concernées. Il est alors important de savoir comment cette sécurité peut être appliquée à un ensemble hétérogène de données et d'applications et donc de déduire quelles lignes de gouvernance il est possible de mettre en œuvre.

I. Les problématiques

La prise en compte par les collectivités territoriales de la sécurité des systèmes d'information ne peut se concevoir qu'à partir du moment ou les responsables des dites collectivités sont conscients qu'ils ont à relever quatre défis : L' e-administration, l' e-démocratie, la dématérialisation des appels d'offres et la mise en place de portails internet. Le développement de l'outil informatique au sein des collectivités territoriales est une réalité. Une étude réalisée en 2010 auprès de plusieurs collectivités territoriales (mairies, conseil régionaux, conseils généraux etc.) de la région du Nord-Pas-de-Calais montre que la prise en compte de la sécurité des systèmes d'information est très faible ; et plus grave encore, que les obligations légales à mettre en œuvre sont dans une grande majorité ignorées des décideurs et responsables.

Les collectivités territoriales présentent une grande

diversité de traitements informatiques, due non seulement à l'existence de différentes entités institutionnelles mais aussi aux rapports entre l'administration et les citoyens ainsi qu'avec le tissu économique local.
Pour les collectivités territoriales, l'écueil principal réside dans le caractère hétérogène des différents fichiers comportant des informations personnelles sur les administrés que la collectivité doit gérer.
Le deuxième point, et non le moindre, concerne les différentes obligations légales à respecter relativement au traitement des dits fichiers.
L'hétérogénéité des fichiers vient du fait que les collectivités territoriales sont soumises au traitement de données à caractère personnel, non seulement dans le cadre des traitements de gestion interne[1], mais également de traitement à caractère administratif[2] ou social[3].
Il pèse donc sur toutes ces entités des obligations légales issues des différents textes que sont : la loi du 6 janvier 1978 dite loi informatique et libertés[4], la loi du 5 janvier 1988 dite loi Godfrain[5] et enfin la loi du 21 juin 2004 intitulée loi pour la confiance dans l'économie numérique[6]. Ces différents textes imposent donc des obligations de sécurité pour le responsable du traitement des données à caractère personnel qu'est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.
Depuis plusieurs années, on constate une volonté des tribunaux de responsabiliser de plus en plus la personne morale (collectivité territoriale) et donc ses responsables sur les problèmes de sécurité informatiques. Un défaut de sécurisation du système d'information peut se traduire soit par un comportement délictueux d'un agent utilisant l'outil informatique mis à sa disposition, soit par une compromission des données personnelles contenues dans les fichiers. Dans les deux cas, il est recherché non seulement la faute commise mais également ce qu'avait fait le responsable pour empêcher la survenance de cette faute.
Une sécurité défaillante pouvant engager la responsabilité tant civile que pénale du dirigeant, la mise en place au sein de la structure d'une sécurité effective des systèmes d'information est primordiale.

II. Des solutions

La mise en place d'une politique de sécurité des systèmes d'information doit partir d'un référentiel. La Direction générale de la modernisation a mis au point, avec la Direction centrale de la sécurité des systèmes d'information un document (référentiel général de sécurité) constituant un outil complet à la disposition du responsable de la sécurité des systèmes d'information (DSI).
Selon la taille de la collectivité territoriale, pourra être mis en place un DSI ou un RSSI, et s'il n'existe aucune possibilité de créer un poste spécifique la sécurité du SI doit correspondre , à minima, à une partie de l'activité quotidienne d'un agent[7].
La définition d'une politique tangible de sécurité ne peut se réaliser que si elle implique l'ensemble des agents et qu'elle obtient un aval politique fort de la part de l'exécutif.
La mise en place d'une politique cohérente de sécurité du système d'information doit s'appuyer sur une participation de tous (sensibilisation des personnels à la sécurité) et sur la mise en œuvre de moyens humains[8] et techniques visant à prendre en compte les différents aspects de la sécurité.
Une des priorités est de s'assurer de l'existence et du suivi d'un certain nombre de documents majeurs dont l'absence serait de nature à retarder toute détection de menace ou de dysfonction-

nement. Il est conseillé tout d'abord de réaliser un triptyque composé du schéma directeur informatique, du plan de câblage et du plan d'adressage consignant l'ensemble des adresses réseaux attribuées et leurs emplacements physiques et logiques. Il sera proposé un tableau de bord en utilisant les préconisations émises par le club de la sécurité des systèmes d'informations français (CLUSIF). Un plan de continuité de l'activité et un plan de reprise d'activité, une charte de bonne utilisation d'Internet et une charte de bonne utilisation de la messagerie pourront compléter le dispositif.
En ce qui concerne l'aspect RH, des séances de sensibilisation doivent être programmées au profit de tous les agents avec des rappels (application des protocoles d'usage de l'outil informatique politique des mots de passe etc..) et des mises en application.
Pour l'aspect technique, il est indispensable de mettre en place le minimum requis pour la protection (antivirus – pare feux, etc.) et d'utiliser au maximum le cryptage des données.

B14 - Lutte informatique défensive et Security Operation Center : vers une cybersécurité dynamique.

Intervenants :

- Solange BELKHAYAT-FUCHS : CNIS,
- Gérard GAUDIN : Consultant (G2C) et président du club R2GS,
- Didier GRAS : Directeur SSI, vice président du forum des compétences, groupe BNP/PARIBAS,
- Elisabeth MANCA : responsable offre sécurité et traitement des menaces, ATHEOS,
- Stéphane LEMEE : Head of SOC, CASSIDIAN CYBERSECURITY,
- Raimund GENES : Chief technology officer, TREND MICRO,
- Gérard OUALID : Responsable du business development des activités sécurité, ALCATEL LUCENT,
- Valéry DEVIANNE : Adjoint OPS au sous-directeur SSI de la DC-DIRISI.

Résumé des interventions :

Si la notion de SOC n'a pas de définition précise, elle peut cependant être distinguée de la prévention.
Au global il importe de retenir que c'est la maturité fonctionnelle des produits SIEM qui est le plus souvent insuffisante et que l'exigence d'une MO qualifiée pour faire face aux menaces est patente.
Par ailleurs, les exigences technologiques importantes traduisent des marges de progression et un club le « R2GS » a pour objectif le partage des meilleures pratiques en France et en Europe.

I. Le constat

La notion de Security Operation Center (SOC) n'a pas de définition fixe. Mais on peut tout de même la distinguer de la « *prévention* » par son aspect dynamique indispensable pour s'adapter en permanence aux menaces et gérer des incidents très fréquents. Le véritable problème des produits SIEM (Security Information Event Management/ Gestion des Evènements et des Informations de Sécurité) serait leur maturité. Une mauvaise appréhension du SIEM comme outil à tout faire peut entrainer son rejet pur et simple par l'organisation. Or, le SOC n'est qu'un outil à utiliser à bon escient : il faut savoir ce que l'on veut en faire à travers une analyse de sécurité complète, identifier ce qu'il faut superviser et quels sont les risques à

éviter en premier lieu. La technologie ne suffit pas en elle-même : il faut de l'audit. Il faut être capable de discerner l'incident qui affectera le business et dans quelles proportions. S'impose ensuite une phase d'élaboration des processus de reporting avec le client, puis une phase de paramétrage relativement simple des outils. Le SOC doit rester proche des réalités de l'entreprise et s'adapter au contexte. C'est pourquoi le SOC relève aujourd'hui du top management et non plus uniquement du RSSI. Les outils qui permettaient, il y a 10 ans de cela, de récupérer les incidents et d'en avertir les administrateurs étaient trop complexes à utiliser et surtout trop lents. Depuis, ces outils ont été couplés à une dimension « *fonctionnelle* » et à de vraies politiques de sécurité pour en accroître l'efficacité.

II. Les solutions

L'existence d'une main d'œuvre qualifiée s'impose pour mieux faire face à des attaques de plus en plus discrètes, ciblées et complexes. Les attaques sont aujourd'hui désignées et structurées pour ne pas être détectées. Pour y répondre, l'analyse humaine des événements de sécurité dans un SOC est un élément crucial. C'est l'analyste qui distinguera les évènements de sécurité importants de ceux qui le sont moins. Et face à une menace furtive, le SOC permet simplement de gagner du temps. Le développement des SOC est cependant confronté au manque de main d'œuvre qualifiée. Combler ce manque à l'aide par des formations adéquates et attractives reste l'un des principaux challenges des prochaines années étant donné la rapidité d'évolution et de sophistication des attaques.
Un SOC performant doit pouvoir s'adapter aux besoins de l'organisation à protéger ainsi qu'a la diversité des formes d'attaques. La qualité de la détection dépend en effet des capacités d'analyse des logs. Il faudra parfois corréler jusqu'à 30 sources différentes d'information, ce que peu d'opérateurs peuvent faire à l'heure actuelle. La fenêtre d'analyse de ces logs sera également susceptible d'évoluer en précision et sur le domaine temporel : d'un mois, elle pourra passer à 6 mois, voire à un an ou plus pour les APT. Or, elle n'est aujourd'hui que d'une journée, la plupart du temps, ce qui pose une réelle difficulté quant à la détection et le suivi des menaces discrètes évoluant pas à pas. La marge de progression en matière de performances technologiques des SOC reste donc relativement importante.
Le club R2GS (réflexion et recherche en gestion opérationnelle de la sécurité) a pour objectif de mettre en partage les pratiques entre les différents professionnels du secteur. Composé de 40 grandes organisations françaises, le club, existant aujourd'hui depuis 4 ans, se développe également dans le reste de l'Europe (Royaume-Uni, Allemagne…) couvrant ainsi un réseau de plus en plus large. De par son important travail sur l'élaboration de standards en matière de SIEM, le club aspire à combler un manque structurel au niveau français, et même mondial. Car il faut des modèles, des référentiels qui lient « *gouvernance* », « *SSI* » et « *terrain* ». Il faut des points de repère, des indicateurs, des références. Pour ce faire, un benchmark s'impose afin de disposer de chiffres fiables et de données de références. La mesure apparait comme la solution permettant d'améliorer la prévention : il faut un observatoire évolutif dédié à ces questions. Sur ce point précis, la France est en retard : il se vendrait trois fois plus d'outils SIEM au Royaume-Uni qu'en France. Un manque de sensibilisation des utilisateurs français sur le sujet serait en cause. Concrètement les chances de succès d'une attaque de type APT sont très minces si l'attaquant ne parvient pas à utiliser le facteur « *humain* ». Rappelons que 70% des incidents de sécurité sont dus à des failles triviales ou à un manque de vigilance.

Les cyber-attaques des réseaux et systèmes d'information sont quotidiennes et de plus en plus sophistiquées. Une approche classique de la sécurité des réseaux n'est plus suffisante. **Prévention, détection et correction** des vulnérabilités en temps réel deviennent un complément indispensable de toute stratégie de cyber-défense efficace.

Les solutions de **cyber-sécurité** et le **Centre Opérationnel de la Sécurité** d'Alcatel-Lucent vous aident à protéger vos réseaux, informations et applications, ainsi qu'à gérer et anticiper en temps réel les menaces en cours ou à venir.

Pour plus d'information, visitez notre site:
www.alcatel-lucent.com

Alcatel·Lucent

AT THE SPEED OF IDEAS™
*À LA VITESSE DES IDÉES™

B15 - BYOD, réseaux sociaux les nouveaux risques en entreprise

Intervenants :

- Jérôme SAIZ
- Eric BARBRY : Avocat à la Cour d'appel de Paris, Directeur du pôle Droit numérique, Cabinet Alain Bensoussan,
- Philippe LOUDENOT : Fonctionnaire de sécurité des systèmes d'information, Service du HFDS auprès du Premier ministre,
- Stéphane OMNES : RSSI, Adeo Services.

Résumé des interventions :

Le cœur du problème est la maîtrise de l'information. Le Byod ne permet pas la maitrise de l'information enregistrée et les réseaux sociaux ne permettent pas de maitriser l'information publiée. Face à cela, la question centrale est la suivante : Est-il possible d'une part de refuser l'usage d'outils numériques personnels pour le travail (Byod) et, d'autre part, d'autoriser l'accès aux réseaux sociaux aux salariés durant leur temps de travail. Si l'on accepte ces mesures, comment gérer leur usage ?

I. Etat des lieux

Le BYOD est interdit dans le service public mais il est autorisé dans certaines entreprises privées. Ainsi, les responsables du secteur privé, qui sont attentifs aux évolutions comportementales de la société, estiment que le BYOD et les réseaux sociaux favorisent le commerce et que les salariés qui utilisent ces ressources y contribuent en qualité d'actionnaires sérieux et responsables de l'entreprise,

Le BYOD a des conséquences cachées qui tiennent au principe d'égalité dans le travail. Le fait que chacun puisse venir avec ses propres outils, plus ou moins sophistiqués, induit une discrimination entre les salariés. Au bout du compte, cela peut conduire à des problèmes sociaux. Un financement des moyens numériques personnels peut être demandé. Dans ces conditions existe-t-il une véritable économie ? Des études montreraient au contraire un surcoût de l'ordre de 30 % des dépenses d'équipement informatique.

Dans le secteur public, tous les agents utilisent le même matériel avec néanmoins pour certaines personnes des services supplémentaires sur leur téléphone de service.

Il existe aujourd'hui un autre modèle économique

qui consiste à écouter le collaborateur et à lui proposer un moyen plus élaboré. Le matériel demeure la propriété de l'entreprise mais il peut être utilisé par le salarié à des fins personnelles pour qu'il reste dans la légalité. Il existe d'ailleurs une forme de suivi, puisque, si un comportement n'est pas conforme à la politique de l'entreprise, un message de mise en garde apparaît à la lecture de l'utilisateur.

L'usage des réseaux sociaux, est autorisé par l'administration car il y a un besoin (ex. les tweets des hommes politiques). Cette opposition « *public-privé* » tient d'abord à la sensibilité de l'information et à la maîtrise des moyens utilisés. Par exemple, les informations relatives au dépouillement d'un appel d'offres ne sauraient être stockées sur un périphérique externe. Elle s'appuie aussi sur le regard différent porté sur les moyens de communication nouveaux et la capacité des salariés.

Dans le secteur privé comme dans le secteur public, il existe une classification des données qui tient compte de leur sensibilité pour un usage particulier. Les uns et les autres motivent leurs collaborateurs sur l'usage des données sensibles. Mais, dans le secteur privé il est plus difficile de faire endosser leurs responsabilités aux directeurs métiers (notamment le marketing) en cas de diffusion de certaines données. En revanche, certains vont veiller naturellement et par principe à les préserver, conscients que leur diffusion pourrait mettre en péril l'entreprise comme par exemple la diffusion des comptes de résultat dans le domaine financier. Pour éviter le stockage intempestif de ces données, il existe dans le secteur privé des solutions techniques qui empêchent un téléchargement local ou sur un terminal. Pour contrôler les orientations données, le secteur privé, a tendance à mettre en œuvre des outils de veille pour juger de sa réputation avec publication d'un rapport annuel.

II. Les solutions juridiques

On peut ne pas adhérer au BYOD et interdire l'accès aux réseaux sociaux sur le temps de travail mais cela devient plus compliquer pour l'interdire sur le temps de pause. L'organisation de l'usage des moyens numériques doit être intégrée dans une charte. Avant d'autoriser l'usage des moyens numériques, il convient de procéder par étape :

1) Autoriser l'emploi des moyens numériques à partir d'une étude de risque social et organisationnel réalisé par le RSSI qui fixera ce qu'il est possible de supporter. S'il existe une réglementation (ex. classification de défense) l'étude sera plus simple. En revanche, en l'absence de texte, il conviendra d'opérer à une classification au cas par cas et éventuellement au fil de l'eau. Dans tous les cas, la direction « métier » décidera de l'autorisation à donner et en assumera les conséquences.

2) Décider des règles d'usage des moyens à partir d'une charte à laquelle seront joints un manuel d'utilisateur technique et un manuel d'utilisation juridique. Cette charte qui fixe les règles d'usage des moyens numériques est bilatérale. Elle engage employeurs et salariés (ex. conservation des données pendant 6 mois et pas au delà).

3) Présenter cette charte pour qu'elle soit opposable aux organes de représentation du personnel, qu'il s'agisse d'un organe public ou d'une entreprise privée.

4) Déclarer à la CNIL les systèmes informatiques correspondants (traceurs, etc.).

5) Sensibiliser et informer les collaborateurs (Charte en ligne).

6) Rédiger un guide des opérations de contrôle interne qui comportera notamment la mise en œuvre de la procédure, ses règles d'action,

comment, avec qui, les autorisations éventuelles du juge.
En cas d'infection du réseau par du matériel personnel comment récupérer le matériel pour analyser le code malveillant et l'attaque?
1) Remise volontaire du matériel. Dans ce cas il n'y a pas de problème.
2) S'il n'existe pas de charte ou, en l'absence de précision de cette dernière, il sera difficile d'agir, sauf menace grave et immédiat (La Cour de cassation ne retient dans l'immédiate qu'un risque terroriste). Pour les autres infractions ce n'est pas possible.
3) Le juge des requêtes. On pourra lui demander d'autoriser la récupération du matériel du collaborateur.

B16 - Le management des professionnels de la cybersécurité

Intervenants :

- Adel JOMNI : enseignant-chercheur, Université Montpellier 1, directeur du diplôme: « Cybercriminalité: Droit, Sécurité de l'information et informatique légale »,
- Philippe LANGLOIS : Président Directeur Général P1 Security,
- Edoaurd JEANSON : Directeur technique de l'activité sécurité, groupe SOGETI,
- Hervé MOLINA : Directeur de l'audit Informatique Groupe, Groupe La Poste,
- Pierre-Luc REFALO : Directeur associé, HAPSIS.

Résumé des interventions :

Devant la difficulté constatée de recruter des experts de la cybersécurité, il faut se questionner sur les spécificités des métiers attachés à cette spécialité, sur les sources et les modes de recrutement, sur l'attractivité du secteur et les moyens de l'améliorer, notamment à travers l'image des métiers de la sécurité informatique et les modes de management utilisés.

I. Les problématiques

Les métiers de la cybersécurité sont multiples et variés : consultants, responsables de la politique de sécurité dans le domaine organisationnel ou d'audits et de tests d'intrusion, professionnels chargés des implémentations de solutions, ceux qui travaillent dans les Security Operating Center (SOC), qui alertent sur les comportements suspects attachés à un métier, ingénieurs-chercheurs... L'ensemble de ces spécialistes œuvrent avec un même objectif mais l'abordent chacun avec un regard différent. Le but est de parvenir à embrasser l'ensemble des problématiques liées à la Cybersécurité.
A l'intérieur même de chacun de ces métiers, de nombreux types de profils différents sont donc requis. On peut les classer en deux catégories : d'un côté les gestionnaires, dont les missions principales sont de gérer et de surveiller les réseaux et de (manager) les équipes; coordonner d'un autre côté, les créatifs, qui s'investissent dans la recherche, dans la mise en œuvre d'une nouvelle architecture de sécurité, dans le forensique et possèdent une aptitude au dépassement. Le management consiste donc à parvenir à articuler ces profils distincts mais complémentaires dans une même équipe et de déterminer les indicateurs permettant d'en mesurer l'efficacité. Les compétences demandées sont nombreuses et le « savoir-être » aux être privilégié au « savoir-faire », même si la partie technique est importante. Ainsi doivent être recherchées des personnes ayant le sens de l'écoute, un esprit d'analyse et de synthèse, des capacités de communication orale et écrite, de la curiosité,

de la rigueur et un comportement éthique. Détecter des failles de sécurité ne suffit pas : il faut pouvoir expliquer intelligiblement en quoi elles représentent un risque et comment y remédier.
De plus, la défense des systèmes d'information des entreprises privées et organismes publics est une activité de service et, à ce titre, exige passion, vocation et sens de l'intérêt général, en dehors de tout opportunisme ou intérêt financier .
La pénurie des compétences et les difficultés de recrutement constatées dans le domaine de la cybersécurité, alors que paradoxalement le métier d'informaticien est désormais touché par le chômage, peuvent avoir plusieurs origines :
- le décalage entre les offres et les demandes de compétences : le domaine de la cybersécurité, où la réactivité est essentielle, peut poser un problème de gestion de temps. En effet, il faut pouvoir trouver le profil adéquat au bon moment, apporter au client l'expertise attendue sur un sujet pointu (Cloud, APT, mobilité, SCADA, etc.) au moment où il en a besoin;
- un nombre insuffisant d'étudiants inscrits dans les masters de cette discipline. Le manque de vocation et la moindre attractivité de ces professions sont souvent cités comme les raisons de cette insuffisance. Les politiques de ressources humaines pratiquées dans certaines SSII ne proposent pas une bonne visibilité sur l'évolution des carrières et sont aussi parfois réticentes à appliquer des critères de recrutement non standards. Elles constituent un frein à un engagement professionnel dans ces filières. Les spécialistes de la sécurité sont très mobiles, quittant facilement une entreprise pour une autre car, dans ce milieu, beaucoup se connaissent et communiquent entre eux. Une société où les conditions de travail sont jugées mal adaptées aux exigences des métiers de la sécurité numérique aura des difficultés pour recruter;
- les salaires peuvent aussi constituer un handicap dans le recrutement de ces spécialistes et particulièrement dans la fonction publique où il est difficile de s'aligner sur les salaires pratiqués par certaines entreprises appartenant au secteur privé, même si l'ANSII propose actuellement des salaires qui sortent de la grille de la fonction publique.

II. Des solutions

Pour pallier cette insuffisance de recrutement et de compétences attendues, plusieurs solutions sont envisageables. Tout d'abord il serait utile de créer un référentiel commun des métiers-fonctions, auquel certaines entreprises travaillent d'ailleurs actuellement, pour permettre de modéliser et de bien identifier chaque rôle, chaque fonction et proposer ainsi une vue d'ensemble du secteur. Il faut veiller à constituer des équipes dynamiques, possédant un très bon niveau d'expertise et une ambiance positive, car, selon un cercle vertueux, les bons éléments attirent les bons éléments. Il faut également adopter une démarche pro-active et se déplacer dans les écoles pour communiquer sur son métier et pour repérer les meilleurs.
Néanmoins, il peut être judicieux, selon les solutions de sécurité recherchées, de recruter des personnes aux parcours moins académiques comme par exemple, et ce ne devrait plus être un tabou, d'anciens hackers. Si l'image de ces derniers est devenue négative, car ils sont associés aux opérations d'intrusions informatiques, ils sont pourtant assez créatifs et innovants. Ils possèdent une qualité unique et précieuse de compréhension organique et non pas systémique des systèmes, apportant ainsi une valeur ajoutée certaine. Pour pouvoir défendre au mieux un

système, il est nécessaire d'être capable de connaître les modes d'attaque et de les anticiper. Ils sont donc les plus à même de concevoir les moyens de protection idoines. Si ce choix de recrutement comporte toujours des risques, il est possible de s'en prémunir en partie, par le recours à la méthode du « screening », qui consiste à détecter les éventuelles menaces, à déterminer si les valeurs du candidat correspondent au poste, afin de s'assurer qu'il n'est pas susceptible d'être compromis, par ego ou appât du gain. Le profil singulier de ces experts demande une forme de management différente : il faut être à leur écoute, être capable de réagir rapidement à leurs découvertes, ne pas leur opposer de contraintes de temps au risque de les voir proposer leurs services à une autre entreprise. Mais s'il est recommandé, dans le cadre de la sécurité opérationnelle, de mettre en place des indicateurs pour détecter qui peut être compromis, volontairement ou involontairement, il est également indispensable d'accorder sa confiance à ses collaborateurs et de travailler dans un respect mutuel.

L'élargissement des recrutements aux candidats étrangers constitue une piste de réflexion supplémentaire pour résoudre le problème de la pénurie des compétences. Cette solution est déjà adoptée dans plusieurs pays. La question des salaires devrait également être prise en considération dans le recrutement afin de fidéliser et rendre le métier plus attractif.

D'une manière générale, il faudrait améliorer la communication sur les métiers de la sécurité informatique afin de diffuser une image positive et moderne.

La formation est aussi au cœur de la problématique de la pénurie des compétences. Il est urgent de l'améliorer afin qu'elle s'adapte à ces nouveaux métiers qui reposent sur des connaissances et des compétences très variées (techniques, juridiques, sociologiques, etc.). Un rapprochement entre le milieu académique, industriel et judiciaire est indispensable pour définir les contenus pédagogiques des formations et mieux anticiper les besoins des entreprises en termes de compétences.

La formation interne et continue au sein des entreprises doit être renforcée afin de pérenniser les emplois dans ce secteur, faciliter les progressions de carrière, faire en sorte que les professionnels de la cybersécurité restent en permanence à leur plus haut niveau. Pour ceux qui sont déjà à la pointe de leur expertise, maintenir leurs compétences par une participation à des colloques, à des challenges à titre personnel, leur donner les moyens d'exercer une veille technologique, d'expérimenter des solutions dans des laboratoires de recherche. Ces actions nécessitent, certes, un important effort d'investissement de la part des entreprises.

Enfin, la sensibilisation des jeunes, dès le collège, aux risques et à la sécurité numérique permet de leur transmettre des connaissances et des valeurs d'éthique dès le plus jeune âge. Cette sensibilisation pourrait jouer un rôle important dans l'amélioration de la notoriété de ces métiers et susciter des vocations.

B17 - La cybercriminalité, un risque assurable ?

Intervenants :

- Jean-Philippe BICHARD : journaliste,
- Jean-Laurent SANTONI : président de Clever Courtage,
- Stéphane JANICHEWSKI : directeur de l'activité sécurité, groupe SOGETI,
- Jérôme GOSSE : expert, Zurich France,
- Alessandro LEZZI : responsable TMB, BEAZLEY.

Résumé des interventions :

Après une prise de conscience tardive des risques, les assureurs proposent désormais une couverture par des offres dédiées, le risque passant désormais pour « assurable ». L'objet du « risque » étant la société chargée de l'exécution du marché, l'approche « couverture du risque » apparaît, au sein du vieux continent trop parcellaire.
C'est pourquoi la réponse à cette problématique, essentiellement liée à la perte de chiffre d'affaires, est bivalente, technique et organisationnelle, et son remboursement fondé sur le forfait.

I. Le consensus

La majeure partie des acteurs présents s'accorde à reconnaître que le marché et l'ensemble des couvertures y afférent apparaissent peu attractifs.
Aussi, est-il nécessaire de donner confiance aux assureurs quant à l'appréhension de ces réalités et de leur proposer des recommandations.
Une nouvelle fois dans le domaine de la cybersécurité s'inscrit en pré-requis de référence la notion de confiance. Une autre interrogation est relative au niveau de risque accepté et acceptable? Dans ce domaine très évolutif, l'adaptation des systèmes de défense doit être permanente et la limite de l'assurabilité ne trouve qu'une seule frontière : la fausse déclaration.

II. Les attentes

L'exemple provient d'une compagnie d'assurances spécialisée « BEAZLEY » dont l'expertise acquise outre-atlantique peut être transposée au sein de l'UE. Dans le cadre de l'identification du risque, une seule entité pour l'heure apparaît comme impactée : la société en charge du marché et de son exécution. Si l'approche des risques est un enjeu majeur pour les années à venir, en cohérence avec la valeur des pertes et vols de données et d'objets, elle n'en demeure pas moins embryonnaire pour l'heure sur le vieux continent. Une étude diligentée par la

compagnie « ZURICH » montre à ce sujet, que seules 15% des entreprises évaluées ont mis en place un département dit de « risk management ».

III. Les enjeux

Les nouvelles menaces, par leur caractère protéiforme et leur propension à percer et toucher l'intégrité des savoirs des entreprises à l'instar de la propriété intellectuelle, induisent au niveau des directions générales une réelle prise de conscience. Dès lors se pose une question principale, quelle est la compatibilité entre assurabilité et intérêt à l'assurance ? La réponse à cette question se veut positive, car tous les risques liés à la divulgation en général impliquent des pertes financières en termes de chiffre d'affaires.
Aussi, la réponse managériale au risque est donnée comme bivalente, technique et organisationnelle.
Dans le modèle mondial qui gouverne l'information, la valeur d'une donnée est liée à sa sensibilité.
Les exemples les plus récents d'attaques virales (SONY/ARAMCO) permettent de conclure que bien souvent il n'existe aucune clause relative aux pertes de chiffre d'affaires. Les remboursements de ces attaques se cantonnent en principe à une valeur forfaitaire définie au moment de la signature des contrats et souvent très éloignée de la réalité du préjudice subi.

B18 - Open data, libération des données publiques et sécurité

Intervenants :

- Gaël MUSQUET : Président d'OpenStreetMap France - Chargé de Mission Cartes & Données libres, Agence Numérique d'Ile-de-France,
- Joël TIGNON : Chef du service Information Géographique et Analyse Spatiale, Conseil régional du Nord-Pas de Calais - Direction du Développement Durable, de la Prospective et de l'Évaluation,
- Alexandre DESROUSSEAUX : Chargé de mission expert, Conseil Régional Nord-Pas de Calais.

Résumé des interventions :

Si l'ouverture et le partage des données publiques recèlent des potentialités considérables, cette manne d'informations peut être exploitée à des fins malveillantes. Qu'il s'agisse des enjeux juridiques encadrant les données personnelles ou de l'exploitation de données libres dans des contextes cybercriminels ou conflictuels (localisation de cibles critiques, etc.), les risques sont présents et doivent être pris en compte par les différents acteurs de l'Open data.

I. Des Problématiques

La problématique de libre circulation des données publiques (collectivités, services centraux de l'État, tout organisme public, etc.) pose la question de leur sécurité face aux prédateurs grâce au libre accès des données.
L'open data désigne le mouvement visant à rendre accessible à tous, via le web, les données publiques non nominatives, ne relevant ni de la vie privée, ni de la sécurité, et collectées par les organismes publics.
La loi n°78-753 du 17 juillet 1978, portant diverses mesures d'amélioration des relations entre l'administration et le public, pose le cadre légal tant du secteur privé que public. Ne sont réutilisables que les informations qui sont librement accessibles, c'est à dire ne faisant pas l'objet de restrictions du droit d'accès énumérées à l'article 6 de la loi et non protégées par le secret.
Les administrations qui détiennent des données publiques, ne sont pas, dans leur majorité, préparées à les diffuser. En effet, le choix des informations et leur mise en forme sur l'open data sont complexes et coûteux. Ce travail prospectif procède des enjeux de l'offre et de la demande. Quels que soient les domaines concernés par la mise en réseau (aménagement, politique sociale, libertés publiques, etc.) le process de

mise à disposition implique plusieurs niveaux d'expertise (recensement des données, audit sur l'état documentaire, étude des fréquences de communication, rédaction, etc.).
Les conditions de mise en œuvre des données ouvertes divergent. Certains pensent qu'il faut donner la priorité aux données qui profiteront à toute la société. Dans ce cas, la règle de communication donne la primauté à l'objet. Dans d'autres cas, les données sont répertoriées et rationalisées par des acteurs privés ou des ONG pour en faire des outils de développement sur le marché.
Par exemple, pour en faire des « killer applications », c'est à dire des programmes informatiques qui justifient à eux seuls, pour de nombreux consommateurs, l'achat ou l'adoption d'un type particulier d'ordinateur, de console de jeu, de système d'exploitation ou de téléphone mobile.
Des rapprochements entre les logiques économiques et les besoins sociaux sont possibles. Par exemple, depuis 10 ans, la Fing (Fondation Internet nouvelle génération) aide les entreprises, les institutions et les territoires à anticiper les mutations liées aux technologies et à leurs usages. Elle a construit un nouveau genre de think tank, dont les productions sont largement reconnues en Europe et ailleurs. Ainsi, cette fondation propose aux collectivités un pacte européen de promotion et d'investissement dans les infrastructures sociales, leviers de la croissance et de la confiance. L'open data permet alors l'accès aux biens publics historiquement produits et garantis par les États et les administrations des pays[1].

1 - Le pacte européen de promotion et d'investissement dans les infrastructures sociales prévoit que l'union européenne doit promouvoir des infrastructures sociales, grâce à des organisations diversifiées, de marché, publiques et de coopération collective.

II. Des solutions

Il faut, dès lors, mettre en avant le cadre juridique qui garantit l'utilisation des données, à savoir, la « licence ». Dans ce contexte, les données ne peuvent pas être librement diffusées ou doivent faire l'objet d'une anonymisation préalable. En dehors de ces exceptions, différents organismes ont élaboré des « licences libres » applicables à tout type de contenu, des origines publiques aux créations de l'esprit.
Il s'agit alors de simples modèles de licence d'exploitation qui n'imposent pas de conformités impératives (sauf en cas d'acte de commerce). Des contrats inédits peuvent être élaborés, à la condition de respecter le droit interne, tant au regard des dispositions des lois du 17 juillet 1978 ou encore de la loi informatique et libertés du 6 janvier 1978, qu'au regard des règles d'ordre public.
En initiant des systèmes de licence réutilisables des données publiques, l'APIE (Agence du Patrimoine Immatériel de l'État) pourrait permettre aux petits acteurs d'obtenir une licence moins onéreuse. Cela permettrait de réduire les risques de déséquilibre entre les acteurs sociaux et la création de lobbies.
En résumé, pour garantir l'équilibre de la balance, il importe que tous les acteurs fassent preuve de bienveillance et d'attention pour limiter tous les risques liés à la transparence et à l'usage abusif des données publiques ouvertes.

B19 - Développer des réseaux de résilience à l'échelon territorial.

Intervenants :

- Jean Fabrice LEBRATY : professeur de sciences de gestion à l'Université de Lyon 3,
- Rémy FEVRIER : Commandant (gendarmerie nationale) maître de conférence associé Université de Paris 1,
- Bruno PIETRINI : chargé de mission, expert DRESTIC conseil régional du Nord Pas-de-Calais,
- Franck TOGNINI : Directeur régional CEIS Nord Pas-de-Calais.

Résumé des interventions :

La résilience représente la capacité pour un organisme à traverser une crise importante tout en conservant sa cohésion. Aujourd'hui, les collectivités territoriales font face à un défi de grande ampleur. En effet, elles sont confrontées à une double contrainte : mettre en œuvre des procédures de dématérialisation dans leurs échanges internes et externes tout en se protégeant des menaces informationnelles insidieuses et souvent inédites pouvant mettre en péril leur fonctionnement.

I. Les problématiques

Depuis plusieurs mois, les médias mettent en avant les atteintes portées aux réseaux informatiques soit de ministères, de préfectures, de mairies, ayant le plus souvent pour conséquence un simple détournement de la page web du dit organisme. Cependant, ces attaques de premier niveau n'excluent pas une possibilité de destruction ou de compromission des données stockées. Face à cette réalité, il est important de prendre conscience du fait que les collectivités territoriales sont des cibles potentielles d'attaques et que, face à ce type d'agression, elles doivent maintenir le bon fonctionnement de leurs différents services, face à des citoyens de plus en plus au fait des risques et de plus en plus exigeants. Le Français est devenu un consommateur de l'internet, dans sa vie de consommateur mais également dans sa vie de citoyen. Il attend de plus en plus de services via internet de la part de l'administration et des collectivités territoriales. En même temps, il est de plus en plus informé des risques de l'utilisation de l'outil numérique[1] et n'accepte pas qu'une panne informatique puisse perturber son quotidien et ses relations avec les services administratifs.

Face à cette obligation de devoir maintenir une activité quasi normale, même en cas de problème infor-

1 - Selon deux sondages de 2010 et 2012, 75% des français craignent l'utilisation d'informations personnelles par un tiers – 79% des français considèrent que la sécurité n'est pas garantie sur les sites administratifs et 77% pensent qu'il est risqué d'enregistrer des informations sur ces sites.

matique, du à une attaque ou à un incident (tremblement de terre, inondations, incendie, etc.), la problématique du positionnement de la direction des systèmes d'information (DSI) est importante au sein du réseau territorial. Car, même si le caractère stratégique de la sécurité de l'information est reconnu, il s'avère que, dans les faits, la présence du DSI est souvent oubliée dans les différents comités de direction composant l'entité territoriale. De même la DSI n'aura pas d'efficacité s'il elle n'est reconnue que par sa compétence technique. Elle doit aussi avoir une légitimé au sein de l'organisme.
L'une des problématiques majeures du développement de réseaux de résilience à l'échelon territorial vient du fait qu'un réseau est composé de partenaires, et qu'au niveau territorial, les différentes entités (administrations, collectivités) ne connaissent pas du tout les partenaires susceptibles de faire partie de ce type de réseau.
Enfin, en France, les organismes ont tendance à mettre en place de nombreuses procédures et méthodes pour ne pas subir une crise. En fait, il serait plus pertinent que l'organisation soit capable en elle même de réagir face à un problème. Mieux vaut être en mesure de rattraper l'erreur qui se produit que de tout faire pour éviter cette erreur.

II. Des solutions

La première chose à prendre en compte pour développer un réseau de résilience à l'échelon territorial est de bien percevoir l'importance de cet échelon. Dans le domaine de la sécurité informatique, il y a encore quelques années, les attaques (ou les incidents) touchant les réseaux étaient plus orientés sur des cibles nationales (ministère, grande société) ou internationales (état, grands opérateurs). De nos jours, la plus petite mairie peut être l'objet d'une attaque. Les exemples ne manquent pas. De plus, à l'échelon territorial, une grande partie de la population se sent concernée car elle est directement impactée.
Il s'agit donc, dans un premier temps, de sensibiliser les collectivités territoriales à l'importance de mettre en place un réseau de résilience permettant de continuer une partie de l'activité malgré la crise à surmonter. Pour cela, il est important de mettre en avant deux leviers concernant le représentant de la collectivité : tout d'abord, en cas de problème (perte de données, compromission), sa responsabilité pénale peut être mise en œuvre si les mesures utiles et nécessaires n'ont pas été respectées. Ensuite, les citoyens sont de plus en plus exigeants face aux demandes de services et ces citoyens sont aussi des électeurs (la sanction pourrait venir des urnes). Enfin, un réseau de résilience bien adapté est un gage de sécurité et peut donc être utilisé comme un argument pour attirer de nouvelles entreprises sur le territoire, cet aspect devenant un atout pour la collectivité ayant fait un effort dans ce domaine.
Une fois les dirigeants sensibilisés et persuadés de l'utilité de ce réseau, il faut faire le point des différents partenaires, les réunir autour d'une table et, sous l'égide de la DSI, mettre en place des liens entre les partenaires. Il peut être utile de créer une cellule de crise regroupant les personnes détenant les compétences. S'agissant des compétences, il apparaît important que la collectivité territoriale, dans les critères de recrutement de ce personnel (et pas seulement des spécialistes), mette en avant un besoin de formation dans le domaine de la sécurité des systèmes d'information.
Afin de permettre à toutes les collectivités territoriales de pouvoir bénéficier de l'apport de ce réseau, on peut envisager des systèmes de

mutualisation permettant plus facilement une continuité et une reprise d'activité en cas de crise[2].

A l'instar de ce que préconise le gouvernement allemand, pourquoi ne pas imaginer l'utilisation des réseaux sociaux comme vecteurs de continuité du service? En effet, si l'on analyse la situation de façon objective, un opérateur comme facebook, face à une attaque massive, réussit à reprendre son activité au bout de quelques jours (au plus). Celles de nos préfectures, qui en ont été victimes, ont mis plusieurs semaines pour reprendre leur activité. Bien sur, dans ce cas, toutes les données ne transiteront pas sur le réseau de secours mais il permettra une activité en mode dégradé.

2 - Dans certaines régions, le maillage des collectivités territoriales a permis par la mutualisation des moyens de sauvegarde de toujours avoir un site en « dehors » de la crise pour assurer une continuité.

MANUEL VALLS
MINISTRE DE L'INTÉRIEUR

FLEUR PELLERIN
MINISTRE DÉLÉGUÉE AUPRÈS DU MINISTRE DU REDRESSEMENT PRODUCTIF, CHARGÉE DES PETITES ET MOYENNES ENTREPRISES, DE L'INNOVATION ET DE L'ÉCONOMIE NUMÉRIQUE

Communiqué de presse

Au Forum International de la Cybersécurité, Manuel VALLS et Fleur PELLERIN posent les bases d'une action commune pour l'usage d'internet en toute sécurité

Lille, le 28 janvier 2013

Manuel VALLS et Fleur PELLERIN ont clôturé le Forum International de la Cybersécurité (FIC), qui s'est déroulé à Lille, les 28 et 29 janvier 2013.

A l'occasion de cet événement international, Fleur PELLERIN a réaffirmé sa volonté de garantir un Internet libre, ouvert et sûr. Elle a rappelé que le secteur de la cybersécurité est décisif pour notre pays, et qu'il doit se structurer pour gagner en visibilité à l'international. La ministre a salué plusieurs fleurons français, et a souligné la nécessité d' « encourager ces entreprises à grandir et conquérir de nouveaux marchés, notamment étrangers, dans le respect, bien évidemment, de nos valeurs fondamentales ».

Fleur PELLERIN a également rappelé l'importance des mesures prises par le Gouvernement pour assurer et renforcer la confiance dans l'économie numérique, notamment dans le domaine de la sécurisation des moyens de paiement.

La ministre a enfin annoncé le lancement d'un projet d'identité numérique. Dans le cadre des investissements d'avenir, l'Etat, le Groupe La Poste, Euro-Information (Groupe Crédit Mutuel/CIC), ainsi que PagesJaunes et SFR se sont unis pour créer la société Idénum. Sa mission sera de fédérer en France le plus grand nombre d'acteurs du numérique autour de référentiels communs et de solutions d'identités numériques universelles. Pour la ministre, l'objectif est de « préserver notre souveraineté nationale face aux alternatives étrangères et non sécurisées ».

Manuel VALLS a souligné la nécessité de développer la coordination entre pays pour mieux répondre à une cybercriminalité organisée, diversifiée et structurée au niveau mondial.

Pour ce faire, le ministre de l'Intérieur a insisté sur la nécessité de mieux connaître ce phénomène et a rappelé la création, à l'occasion de la refonte de l'outil statistique,

d'un indicateur spécifique à la cybercriminalité. En outre, le déploiement de nouveaux logiciels d'enregistrement des plaintes dans les commissariats et gendarmeries, ainsi que la généralisation de la plainte en ligne, vont contribuer à quantifier et à qualifier cette délinquance.

Un diagnostic précis est nécessaire pour construire une politique de sécurité efficace, qui passe aussi par une réflexion sur les critères de recrutement et de formation des enquêteurs, ainsi que par la coordination de l'action de tous les acteurs de la chaîne pénale.

Toutefois, les exigences de la lutte contre la cybercriminalité doivent être conciliées avec le respect des grands principes de notre démocratie : liberté d'expression, garanties de la vie privée et des libertés individuelles.

Manuel VALLS a annoncé la mise en place, au sein du ministère de l'Intérieur, d'un groupe de travail qui aura pour mission de définir, dans un cadre interministériel, les grands axes d'une consolidation de l'action de prévention et de lutte contre la cybercriminalité. Ses conclusions devront lui être remises au printemps.

Contact presse :

Cabinet de Manuel VALLS –
Harold HAUZY, conseiller presse et communication : 01 49 27 38 53

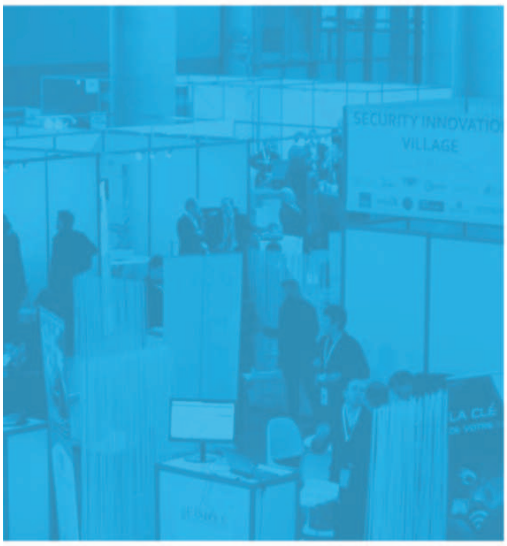
Cabinet de Fleur PELLERIN –
Aziz RIDOUAN, conseiller presse et communication : 01 53 18 41 00

SUIVEZ-NOUS SUR TWITTER

FIC 2013 – Le cyberespace, enjeu de souveraineté et de sé
SUIVEZ-NOUS SUR TWITTER

FIC 2014

IDENTITÉ NUMÉRIQUE ET CONFIANCE



6ème Forum International de la Cybersécurité

21 et 22 janvier 2014
Lille Grand Palais - France

Sous le Haut Patronage de **Monsieur François HOLLANDE, Président de la République**

Un événement co-organisé par

La Gendarmerie Nationale / Le Conseil régional du Nord-Pas de Calais / CEIS